Dimension ES-3024

Ethernet Switch

June 2003

Version 1

User's Guide

ZyXEL
Unleash Networking Power

Copyright

Copyright © 2003 by ZyXEL Communications Corporation

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patents rights of others. ZyXEL further reserES-3024 the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

Trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two (2) years from the date of purchase. During the warranty period and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind of character to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty giES-3024 you specific legal rights, and you may also have other rights that vary from country to country.

Interference Statements and Warnings

FCC Interference Statement

This switch complies with Part 15 of the FCC rules. Operation is subject to the following two conditions:

(1) This switch may not cause harmful interference.

(2) This switch must accept any interference received, including interference that may cause undesired operations.

FCC Warning

This equipment has been tested and found to comply with the limits for a Class A digital switch, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE Mark Warning:

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Taiwanese BSMI (Bureau of Standards, Metrology and Inspection) A Warning:

警告使用者:
這是甲類的資訊產品, 在居住的環境中使用時,
可能會造成射頻干擾, 在這種情況下,
使用者會被要求採取某些適當的對策.

Certifications

Refer to the product page at www.zyxel.com.

Customer Support

If you have questions about your ZyXEL product or desire assistance, contact ZyXEL Communications Corporation offices worldwide, in one of the following ways:

Contacting Customer Support

When you contact your customer support representative, have the following information ready:

- Product model and serial number.
- Firmware version information.
- Warranty information.
- Date you received your product.
- Brief description of the problem and the steps you took to solve it.

METHOD LOCATION	E-MAIL: SUPPORT SALES	TELEPHONE FAX	WEB SITE FTP SITE	REGULAR MAIL
WORLDWIDE	support@zyxel.com.tw sales@zyxel.com.tw	+886-3-578-3942 +886-3-578-2439	www.zyxel.com www.europe.zyxel.com ftp.europe.zyxel.com	ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 300, Taiwan
NORTH AMERICA	support@zyxel.com sales@zyxel.com	+1-800-255-4101	www.us.zyxel.com ftp.zyxel.com	
SCANDINAVIA	support@zyxel.dk sales@zyxel.dk	+45-3955-0700 +45-3955-0707	www.zyxel.dk ftp.zyxel.dk	ZyXEL Communications A/S, Columbusvej 5, 2860 Soeborg, Denmark
GERMANY	support@zyxel.de sales@zyxel.de	+49-2405-6909-0 +49-2405-6909-99	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen, Germany

Table of Contents

Copyright ii
ZyXEL Limited Warranty iii
Interference Statements and Warnings iv
Customer Support v
Preface 15
Features And Applications I
Chapter 1 Getting to Know the ES-3024 1-1
1.1 Features 1-1
1.2 Applications 1-3
Hardware Installation & Connections II
Chapter 2 Hardware Installation 2-1
2.1 Installation Scenarios 2-1
Chapter 3 Hardware Connections 3-1
3.1 Front Panel 3-1
3.2 Uplink Modules 3-2
3.3 Rear Panel 3-4
3.4 Front Panel LEDs 3-4
3.5 Stacking Scenario Examples 3-5
3.6 Uplink Scenario Example 3-7
3.7 Configuring the ES-3024 3-8
Getting Started III
Chapter 4 Introducing the Web Configurator 4-1
4.1 Introduction 4-1
4.2 System Login 4-1
4.3 Switch Lockout 4-2
4.4 Resetting the Switch 4-2
4.5 Home Screen 4-3
4.6 Screen Overview 4-5
Chapter 5 General, Switch and IP Setup 5-1
5.1 Introduction 5-1

5.2 General Setup 5-1
5.3 IGMP Snooping 5-2
5.4 Introduction to VLANs 5-2
5.5 Introduction to Spanning Tree Protocol (STP) 5-2
5.6 Dynamic Link Aggregation 5-4
5.7 802.1X Authentication 5-4
5.8 Switch Setup Screen 5-4
5.9 IP Setup 5-8
Chapter 6 Port Setup 6-1
6.1 Introduction 6-1
6.2 IEEE 802.1x 6-2
6.3 Configure 802.1x on a Port 6-2
Advanced Applications IV
Chapter 7 Static Route Setup 7-1
7.1 Static Route Setup 7-1
7.2 Static Route Edit Setup 7-2
Chapter 8 VLAN Setup 8-1
8.1 Introduction to IEEE 802.1Q Tagged VLAN 8-1
8.2 Configuring Tagged VLANs 8-3
8.3 Introduction to Port-based VLANs 8-6
8.4 Configuring Port-based VLANs 8-6
Chapter 9 Static MAC Forward Setup 9-1
9.1 Introduction to Static MAC Forward Setup 9-1
9.2 Configuring or Editing a Static MAC Forward Rule 9-2
Chapter 10 Filter Setup 10-1
10.1 Introduction to Port Filtering 10-1
10.2 Configuring or Editing a Filter Rule 10-2
Chapter 11 Mirror Setup 11-1
11.1 Introduction to Port Mirroring 11-1
11.2 Configuring or Editing a Mirror Rule 11-2
Chapter 12 Bandwidth Control Setup 12-1
12.1 Introduction to Bandwidth Control 12-1

12.2 Configuring or Editing a Bandwidth Control Rule 12-2
Chapter 13 Trunk Setup 13-1
13.1 Introduction to Trunking 13-1
13.2 Trunk Setup 13-1
Advanced Management V
Chapter 14 SNMP 14-1
14.1 About SNMP 14-1
14.2 Supported MIBs 14-2
14.3 Configuring SNMP 14-2
14.4 SNMP Traps 14-3
Chapter 15 RADIUS Setup 15-1
15.1 Introduction to RADIUS 15-1
15.2 RADIUS Setup 15-1
Chapter 16 Logins 16-1
16.1 Introduction 16-1
Chapter 17 Maintenance 17-1
17.1 Maintenance 17-1
17.2 Remote Management 17-3
Chapter 18 Firmware and Configuration File Maintenance 18-1
18.1 Firmware Upgrade 18-1
18.2 Restore a Configuration File 18-1
18.3 Back Up a Configuration File 18-2
18.4 Command Line FTP 18-2
Chapter 19 Statistics 19-1
19.1 Introduction to Statistics 19-1
Chapter 20 Diagnostic 20-1
20.1 Diagnostic 20-1
Commands VI
Chapter 21 Commands Introduction 21-1
21.1 Command Line Interface Overview 21-1
21.2 Command Summary 21-2
Chapter 22 Command Examples 22-1

22.1 Commonly Used Commands Overview 22-1
22.2 Sys Commands 22-1
Chapter 23 IEEE 802.1Q Tagged VLAN 23-1
23.1 IEEE 802.1Q Tagged VLAN Overview 23-1
23.2 Filtering Databases 23-1
23.3 Configuring Tagged VLAN 23-1
23.4 IEEE VLAN1Q Tagged VLAN Configuration Commands 23-3
23.5 VLAN1Q SVLAN Active Command 23-8
23.6 VLAN1Q SVLAN Inactive Command 23-8
23.7 VLAN1Q SVLAN List Command 23-8
23.8 VLAN1Q VLAN List Command 23-9
Appendices and Index VII
Appendix A Product Specifications 1
Index 4

List of Figures

Figure 1-1 Backbone Application 1-4
Figure 1-2 Bridging Application 1-5
Figure 1-3 High Performance Switched Workgroup Application 1-6
Figure 1-4 VLAN Workgroup Application 1-7
Figure 1-5 Shared Server Using VLAN Example 1-8
Figure 2-1 Attaching Rubber Feet 2-1
Figure 2-2 Attaching Mounting Brackets and Screws 2-2
Figure 2-3 Mounting the ES to an EIA standard 19-inch rack 2-3
Figure 3-1 ES-3024 Front Panel 3-1
Figure 3-2 Loosening the Screws and Removing the Cover Plate 3-3
Figure 3-3 Inserting An Example Module 3-3
Figure 3-4 ES-3024 Rear Panel 3-4
Figure 3-5 Front Panel LEDs 3-4
Figure 3-6 Stacking Example 1 3-5
Figure 3-7 Stacking Example 2 3-6
Figure 3-8 Stacking Example 3 3-7
Figure 3-9 Uplink Example 3-8
Figure 4-1 Web Configurator - Login 4-1
Figure 4-2 Change Password Screen 4-2
Figure 4-3 ES-3024 Home Screen 4-3
Figure 5-1 General Setup 5-1
Figure 5-2 Switch Setup 5-5
Figure 5-3 IP Setup 5-9
Figure 6-1 Port Setup Summary Screen 6-1
Figure 6-2 Port Edit Screen 6-3
Figure 7-1 Static Route Setup 7-1
Figure 7-2 Static Route Edit Setup 7-2
Figure 8-1 VLAN Static Entry Setup 8-3
Figure 8-2 Edit VLAN Static Entry 8-5
Figure 8-3 Port-based VLAN Setup 8-7

Figure 8-4 Port-based VLAN Example 8-8
Figure 9-1 Static MAC Forward Setup 9-1
Figure 9-2 Configuring or Editing a Static MAC Forward Rule 9-2
Figure 10-1 Filter Setup 10-1
Figure 10-2 Configuring or Editing a Filter Rule 10-3
Figure 11-1 Mirror Setup 11-1
Figure 11-2 Configuring or Editing a Mirror Rule 11-3
Figure 12-1 Bandwidth Control Setup 12-1
Figure 12-2 Bandwidth Control Setup Edit 12-3
Figure 13-1 Trunk Setup 13-2
Figure 14-1 SNMP Management Model 14-1
Figure 14-2 SNMP Setup 14-3
Figure 15-1 RADIUS Server 15-1
Figure 15-2 RADIUS Setup 15-1
Figure 16-1 Logins 16-1
Figure 16-2 Edit Logins 16-2
Figure 17-1 Maintenance 17-1
Figure 17-2 Remote Management 17-3
Figure 17-3 Edit Secured Client 17-4
Figure 18-1 Firmware Upgrade 18-1
Figure 18-2 Restore Configuration 18-2
Figure 18-3 Backup Configuration 18-2
Figure 19-1 Statistics 19-1
Figure 19-2 STP Statistics 19-2
Figure 19-3 Aggregator ID: 19-4
Figure 19-4 LACP Status 19-4
Figure 19-5 Hardware Monitor 19-5
Figure 19-6 802.1Q VLAN Status 19-7
Figure 19-7 Port Statistics 19-8
Figure 19-8 Port Details 19-9
Figure 20-1 Diagnostic Screen 20-1
Figure 22-1 Log Disp Command Example 22-1

Figure 22-2 Version Command Example 22-2
Figure 22-3 Monitor Status Command Example 22-2
Figure 23-1 Tagged VLAN Configuration and Activation Example 23-2
Figure 23-2 CPU VLAN Configuration and Activation Example 23-2
Figure 23-3 Deleting Default VLAN Example 23-3
Figure 23-4 GARP Status Command Example 23-3
Figure 23-5 GARP Timer Command Example 23-4
Figure 23-6 GARP Status Command Example 23-4
Figure 23-7 VLAN1Q Port Status Command Example 23-5
Figure 23-8 VLAN1Q Port Default VID Command Example 23-5
Figure 23-9 VLAN1Q Port Accept Command Example 23-5
Figure 23-10 VLAN1Q Port GVRP Command Example 23-5
Figure 23-11 VLAN1Q Port GVRP Command Example 23-5
Figure 23-12 Modifying the Static VLAN Example 23-7
Figure 23-13 VLAN1Q SVLAN Delentry Command Example 23-8
Figure 23-14 VLAN1Q SVLAN List Command 23-9
Figure 23-15 VLAN1Q SVLAN List Command 23-9
Figure 23-16 VLAN1Q Status Command Example 23-10

List of Charts

Chart 1 General Product Specifications 1
Chart 2 Performance and Management Specifications 2
Chart 3 Physical and Environmental Specifications 3

List of Tables

Table 3-1 ES-3024: Front Panel Ports 3-1
Table 3-2 ES-3024 Switches: LED Descriptions 3-4
Table 4-1 Navigation Panel Links 4-4
Table 4-2 Web Configurator Screen Overview 4-5
Table 5-1 General Setup 5-1
Table 5-2 STP Path Costs 5-3
Table 5-3 STP Port States 5-3
Table 5-4 Switch Setup 5-6
Table 5-5 IP Setup 5-9
Table 6-1 Port Setup Summary Screen 6-2
Table 6-2 Port Edit Screen 6-4
Table 7-1 Static Route Setup 7-1
Table 7-2 Static Route Edit Setup 7-2
Table 8-1 GARP Terminology 8-2
Table 8-2 VLAN Static Entry Setup 8-3
Table 8-3 Edit VLAN Static Entry 8-5
Table 8-4 Port-based VLAN Setup 8-8
Table 9-1 Static MAC Forward Setup 9-1
Table 9-2 Configuring or Editing a Static MAC Forward Rule 9-2
Table 10-1 Filter Setup 10-1
Table 10-2 Configuring or Editing a Filter Rule 10-3
Table 11-1 Mirror Setup 11-1
Table 11-2 Configuring or Editing a Mirror Rule 11-3
Table 12-1 Bandwidth Control Setup 12-1
Table 12-2 Bandwidth Control Setup Edit 12-3
Table 13-1 Trunk Groups 13-1
Table 13-2 Trunk Setup 13-2
Table 14-1 SNMP Commands 14-2
Table 14-2 SNMP Setup 14-3
Table 14-3 SNMP Traps 14-3

Table 15-1 RADIUS Setup 15-2
Table 16-1 Logins 16-2
Table 17-1 Maintenance 17-2
Table 17-2 Remote Management 17-3
Table 17-3 Edit Secured Client 17-4
Table 18-1 Filename Conventions 18-3
Table 18-2 General Commands for GUI-based FTP Clients 18-4
Table 19-1 Statistics 19-1
Table 19-2 STP Statistics 19-2
Table 19-3 LACP Statistics 19-4
Table 19-4 Hardware Monitor 19-6
Table 19-5 802.1Q VLAN Status 19-7
Table 19-6 Port Statistics 19-8
Table 19-7 Port Details 19-10
Table 20-1 Diagnostic Screen 20-1
Table 21-1 command summary 21-2

Preface

Congratulations on your purchase from the Dimension series of Ethernet switches.

This preface introduces you to the ES-3024 and discusses the conventions of this User's Guide. It also provides information on other related documentation.

About the ES-3024

The ES-3024 Ethernet switch is a managed switch with features ideally suited in any environment with unshielded twisted pair (UTP) wiring. It can deliver broadband IP services to:

- Multi-tenant unit (MTU) buildings (hotels, motels, resorts, residential multi-dwelling units, office buildings, educational establishments, etc.)
- Public facilities (convention centers, airports, plazas, train stations, etc.)
- Enterprises.

It can also be deployed as a mini-POP (point-of-presence) in a building basement delivering 10/100Mbps data service over Category 5 wiring to each customer.

General Syntax Conventions

- This guide shows you how to configure the switch using the web configurator and CLI commands. See the online HTML help for information on individual web configurator screens.
- Mouse action sequences are denoted using a comma. For example, click **Start, Settings, Control Panel, Network** means first you click **Start**, click or move the mouse pointer over **Settings**, then click or move the mouse pointer over **Control Panel** and finally click (or double-click) **Network**.
- "Enter" means for you to type one or more characters. "Select" or "Choose" means for you to use one of the predefined choices.
- Predefined choices are in **Bold Arial** font.
- Button and field labels, links and screen names in are in **Bold Times New Roman** font.
- For brevity's sake, we will use "e.g." as shorthand for "for instance", and "i.e." as shorthand for "that is" or "in other words" throughout this manual.

Related Documentation

Web Configurator Online HTML help

The online HTML help shows you how to use the web configurator to configure individual screens. More background information can be found in this UG.

ZyXEL Web Site

The ZyXEL download library at www.zyxel.com contains additional support documentation as well as an online glossary of networking terms.

User Guide Feedback

Help us help you! E-mail all User Guide-related comments, questions or suggestions for improvement to techwriters@zyxel.com.tw or send regular mail to The Technical Writing Team, ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 300, Taiwan. Thank you!

Part I

Features And Applications

This part acquaints you with the features and applications of the ES-3024.

Chapter 1
Getting to Know the ES-3024

This chapter describes the key features, benefits and applications of the ES-3024.

The ES-3024 is a stand-alone Ethernet switch with 24 10/100Mbps ports, two slots for electrical or optical uplink modules and one slot for a stacking module.

With its built-in web configurator, managing and configuring the switch is easy. From cabinet management to port-level control and monitoring, you can visually configure and manage your network via the web browser. Just click your mouse instead of typing cryptic command strings. In addition, the switch can also be managed via Telnet, the console port, or third-party SNMP management.

1.1 Features

The next two sections describe the hardware and firmware features of the ES-3024.

1.1.1 Hardware Features

24 10/100 Mbps Fast Ethernet Ports

Connect up to 24 computers or switches to the 10/100Mbps auto-negotiating, automatic cable sensing (auto-MDIX) Ethernet RJ-45 ports. All Ethernet ports support:

- IEEE 802.3/3u/3z/3ab standards
- Back pressure flow control in half duplex mode
- IEEE 802.3x flow control in full duplex mode

Two Slots for Uplink Modules

The modules allow the ES-3024 to connect to another WAN switch or daisy-chain to other switches.

One Slot for Stacking Module

Up to eight switches may be stacked using stacking modules.

Console Port

Use the console port for local management of the switch.

Fans

The fans cool the ES-3024 sufficiently to allow reliable operation of the switch in even poorly ventilated rooms or basements.

1.1.2 Firmware Features

IP Protocols

- IP Host (No routing)
- Telnet for configuration and monitoring
- SNMP for management
  - SNMP MIB II (RFC 1213)
  - SNMP v1 RFC 1157
  - SNMPv2, SNMPv2c or later version, compliant with RFC 2011 SNMPv2 MIB for IP, RFC 2012 SNMPv2 MIB for TCP, RFC 2013 SNMPv2 MIB for UDP
  - Ethernet MIBs RFC 1643
  - Bridge MIBs RFC 1493
  - SMI RFC 1155
  - RMON RFC 1757
  - o SNMPv2, SNMPv2c RFC 2674

Management

- Web configurator
- Command-line interface locally via console port or remotely via Telnet
- SNMP

System Monitoring

- System status (link status, rates, statistics counters)
- SNMP
- Temperatures, voltage, fan speed reports and alarms
- Port Mirroring allows you to analyze one port's traffic from another.

Security

- System management password protection
- IEEE 802.1Q VLAN
- Limit dynamic port MAC address learning
- Port-based VLAN
- 802.1x Authentication
- Static MAC address filtering

Port Trunking

The ES-3024 adheres to the 802.3ad standard for static and dynamic port trunking.

Bandwidth Control

- The ES-3024 supports rate limiting in 1Kbps increments allowing you to create different service plans

- The ES-3024 supports IGMP snooping enabling group multicast traffic to be only forwarded to ports that are members of that group; thus allowing you to significantly reduce multicast traffic passing through your switch.
- Broadcast storm control

Quality of Service

- Four priority queues so you can ensure mission-critical data gets delivered on time.
- Follows the IEEE 802.1p priority setting standard based on source/destination MAC addresses.

STP (Spanning Tree Protocol)

STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a switch to interact with other STP-compliant switches in your network to ensure that only one path exists between any two stations on the network.

1.2 Applications

This section shows a few examples of using the ES-3024 in various network environments.

1.2.1 Backbone Application

In this application, the switch is an ideal solution for small networks where rapid growth can be expected in the near future.

The switch can be used standalone for a group of heavy traffic users. You can connect computers directly to the switch's port or connect other switches to the ES-3024.

In this example, all computers connected directly or indirectly to the ES-3024 can share super high-speed applications on the Gigabit server.

To expand the network, simply add more networking devices such as switches, routers, firewalls, print servers etc.

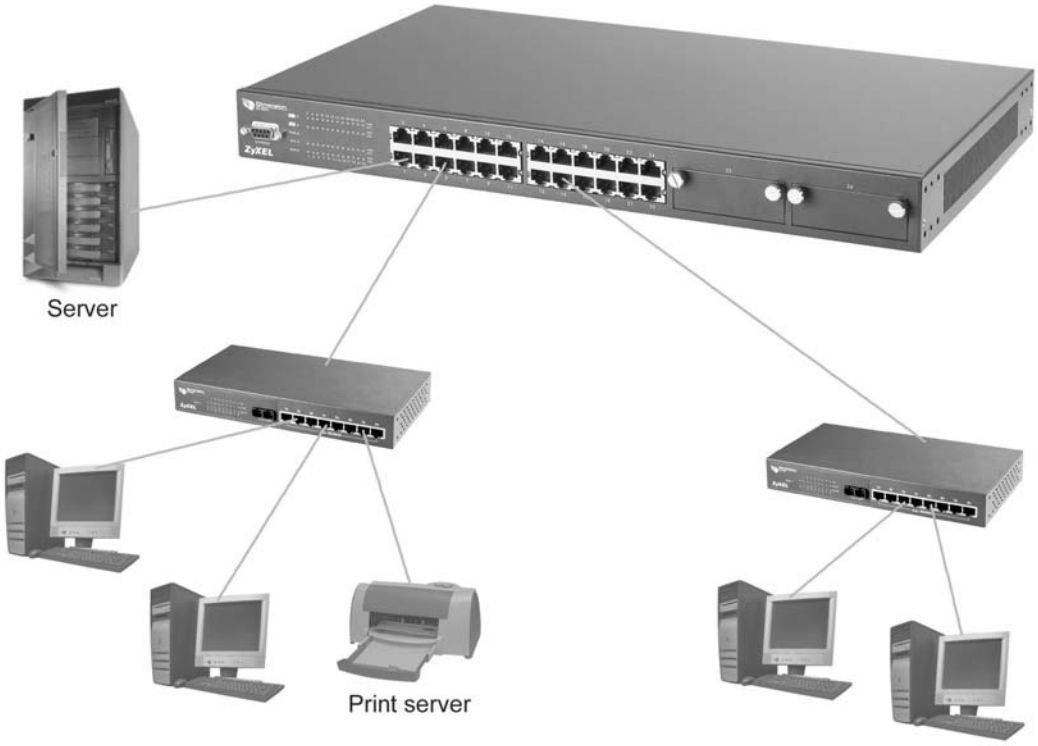

Figure 1-1 Backbone Application

1.2.2 Bridging Example

In this example application the switch is the ideal solution for different company departments to connect to the corporate backbone. It can alleviate bandwidth contention and eliminate server and network bottlenecks. All users that need high bandwidth can connect to high-speed department servers via the switch. You can provide a super-fast uplink connection by selecting from an array of uplink modules compatible with the ES-3024.

Moreover, the switch eases supervision and maintenance by allowing network managers to centralize multiple servers at a single location.

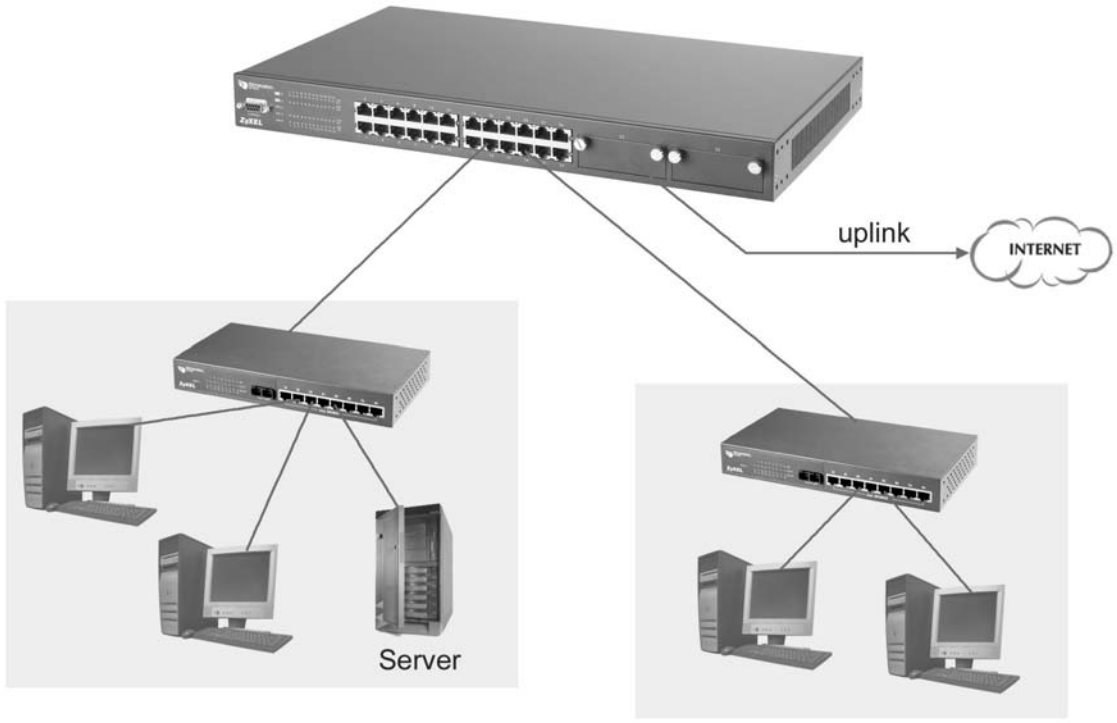

Figure 1-2 Bridging Application

Full-duplex mode operation only applies to point-to-point access (for example, when attaching the switch to a workstation, server, or another switch). When connecting to hubs, use a standard cascaded connection set at half-duplex operation.

1.2.3 High Performance Switched Workgroup Example

The switch is ideal for connecting two power workgroups that need high bandwidth. In the following example, use trunking to connect these two power workgroups.

Switching to higher-speed LANs such as FDDI or ATM is not feasible for most people due to the expense of replacing all existing Ethernet cables and adapter cards, restructuring your network and complex maintenance.

The ES-3024 can provide the same bandwidth as FDDI and ATM at much lower cost while still being able to use existing adapters and switches. Moreover, the current LAN structure can be retained as all ports can freely communicate with each other.

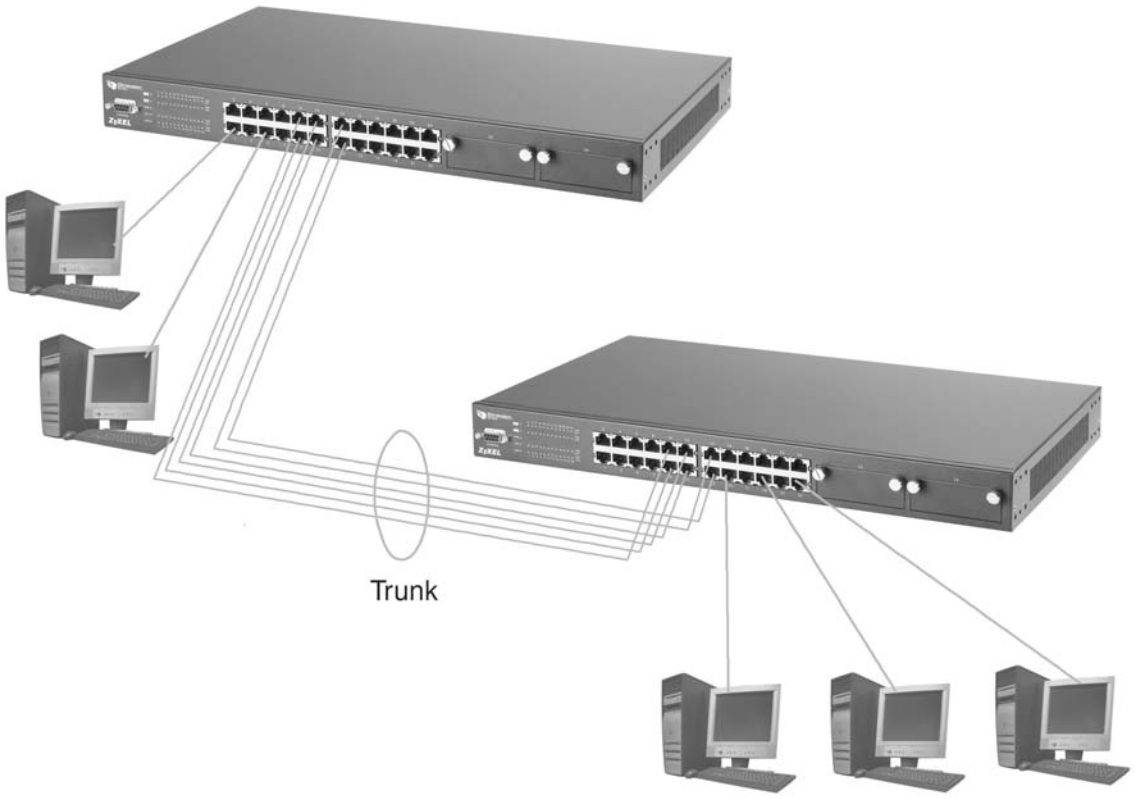

Figure 1-3 High Performance Switched Workgroup Application

1.2.4 IEEE 802.1Q VLAN Application Examples

This section shows a workgroup and a shared server example using 802.1Q tagged VLANs. For more information on VLANs, see the *Switch Setup* and *VLAN Setup* chapters in this User's Guide. A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Stations on a logical network belong to one group. A station can belong to more than one group. With VLAN, a station cannot directly talk to or hear from stations that are not in the same group(s) unless such traffic first goes through a router.

Tag-based VLAN Workgroup Example

Ports in the same VLAN group share the same broadcast domain thus increase network performance through reduced broadcast traffic. VLAN groups can be modified at any time by adding, moving or changing ports without any re-cabling.

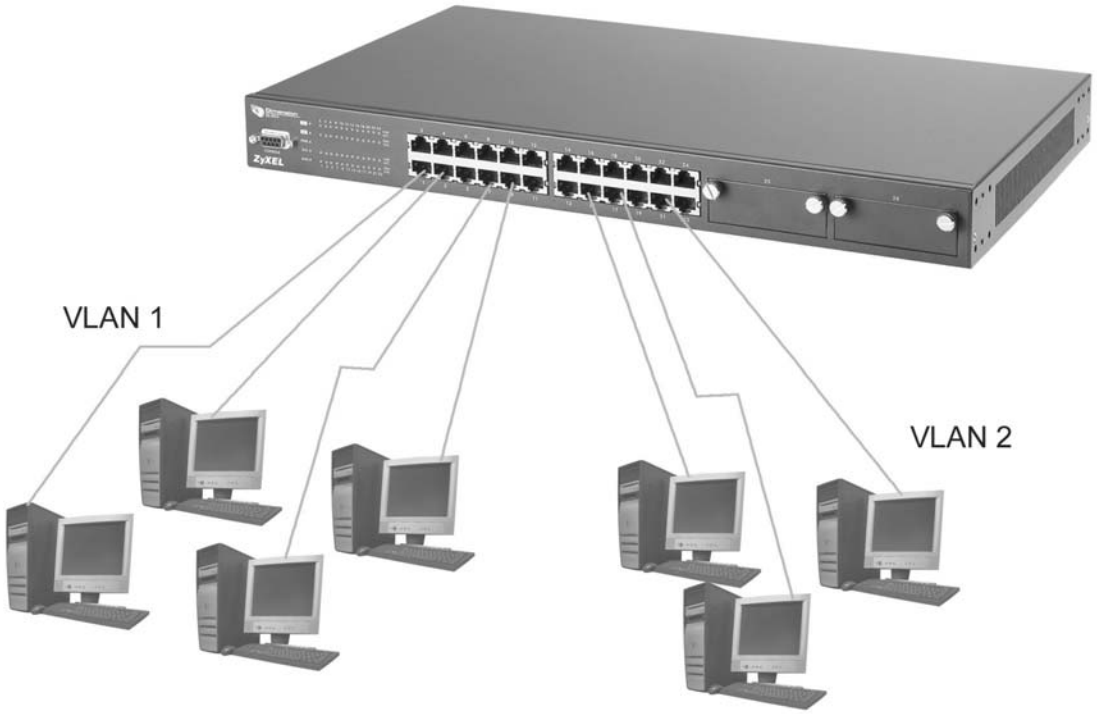

Figure 1-4 VLAN Workgroup Application

VLAN Shared Server Example

Shared resources such as a server can be used by all ports in the same VLAN as the server, as shown in the following example. In this example, only ports that need access to the server need belong to VLAN 3 while they can belong to other VLAN groups too.

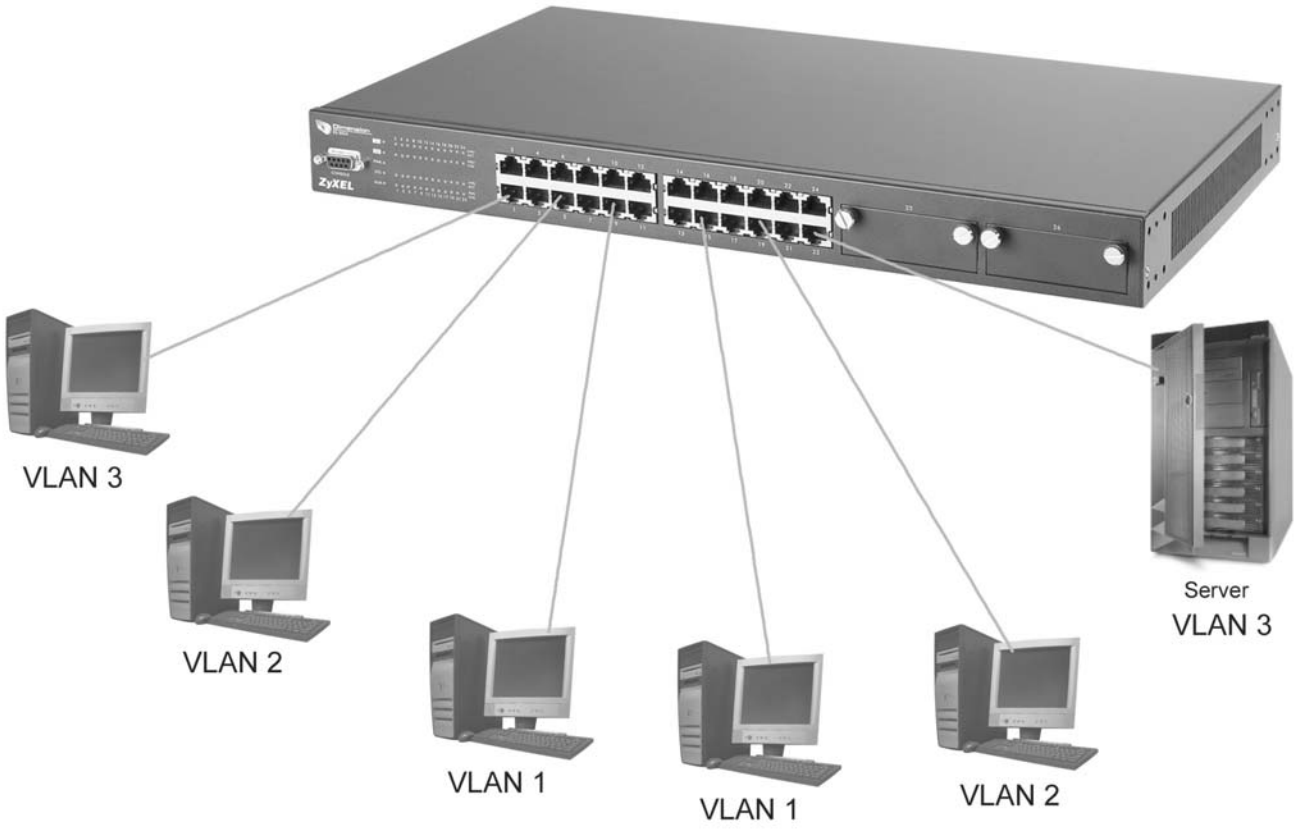

Figure 1-5 Shared Server Using VLAN Example

Part II

Hardware Installation & Connections

This part acquaints you with installation scenarios of the ES-3024, instructs you on how to make the hardware connections including installing/removing modules, shows some stacking/uplink examples and explains the front panel LEDs.

Chapter 2
Hardware Installation

This chapter shows two switch installation scenarios.

2.1 Installation Scenarios

The switch can be placed on a desktop or rack-mounted on a standard EIA rack. Use the rubber feet in a desktop installation and the brackets in a rack-mounted installation.

For proper ventilation, allow at least 4 inches (10 cm) of clearance at the front and 3.4 inches (8 cm) at the back of the switch. This is especially important for enclosed rack installations.

2.1.1 Desktop Installation Procedure

Step 1. Make sure the switch is clean and dry.

Step 2. Set the switch on a smooth, level surface strong enough to support the weight of the switch and the connected cables. Make sure there is a power outlet nearby.

Step 3. Make sure there is enough clearance around the switch to allow air circulation and the attachment of cables and the power cord.

Step 4. Remove the adhesive backing from the rubber feet.

Step 5. Attach the rubber feet to each corner on the bottom of the switch. These rubber feet help protect the switch from shock or vibration and ensure space between switches when stacking.

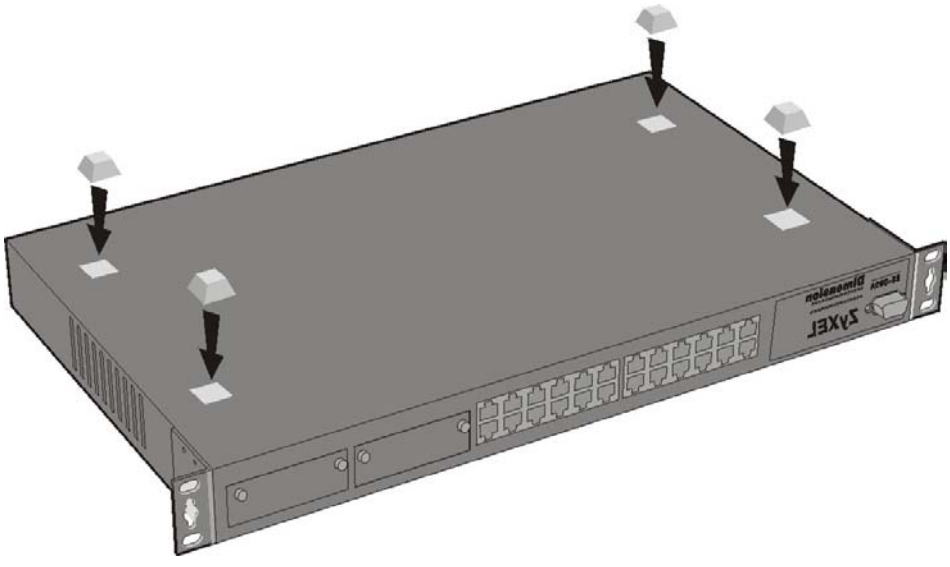

Figure 2-1 Attaching Rubber Feet

Do not block the ventilation holes. Leave space between switches when stacking.

2.1.2 Rack-Mounted Installation

The switch can be mounted on an EIA standard size, 19-inch rack or in a wiring closet with other equipment. Follow the steps below to mount your switch on a standard EIA rack using a rack-mounting kit.

Step 1. Align one bracket with the holes on one side of the switch and secure it with the bracket screws smaller than the rack-mounting screws.

Step 2. Attach the other bracket in a similar fashion.

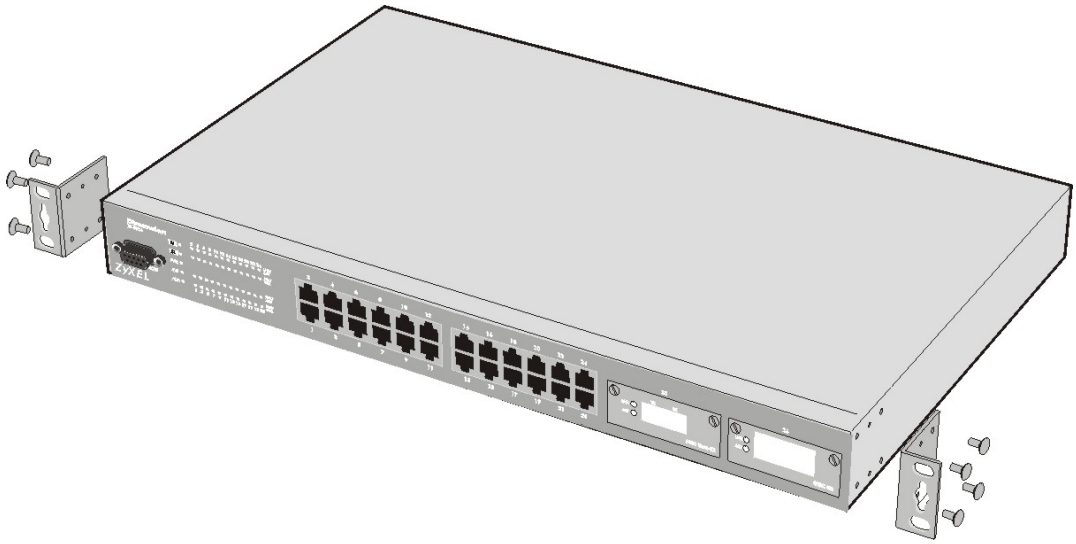

Figure 2-2 Attaching Mounting Brackets and Screws

Step 3. After attaching both mounting brackets, position the switch in the rack by lining up the holes in the brackets with the appropriate holes on the rack. Secure the switch to the rack with the rack-mounting screws.

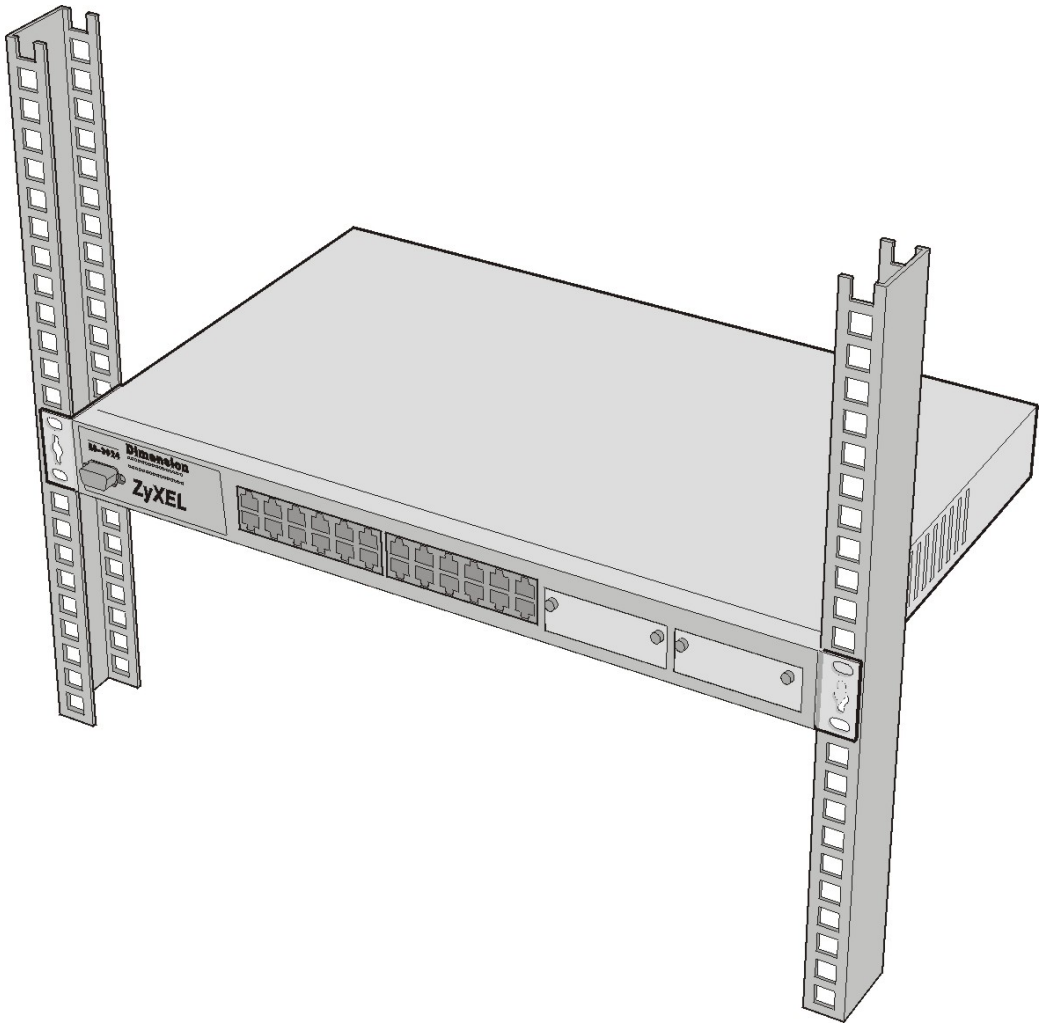

Figure 2-3 Mounting the ES to an EIA standard 19-inch rack

Chapter 3
Hardware Connections

This chapter acquaints you with the front and rear panels, shows you how to make the connections, install/remove (optional) modules and explains the LEDs.

3.1 Front Panel

The following figure shows the front panel of the ES-3024. The front panel contains a console port for local switch management, switch LEDs, 24 RJ-45 Ethernet ports and two (optional) uplink modules.

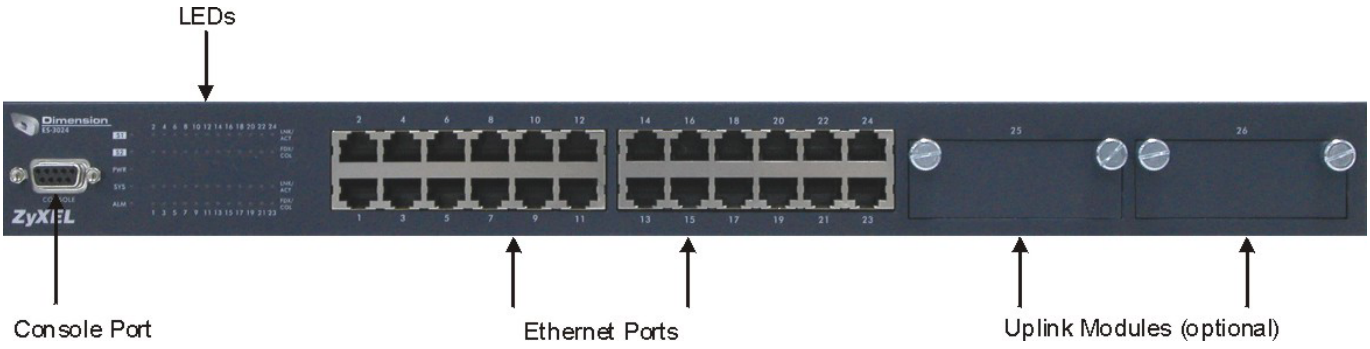

Figure 3-1 ES-3024 Front Panel

Table 3-1 ES-3024: Front Panel Ports

CONNECTOR	DESCRIPTION
Console	The console port is for local configuration of the ES-3024 switch.
24 10/100 Mbps RJ-45 Ethernet connectors	Connect these ports to a computer, a hub, an Ethernet switch or router.

3.1.1 Console Port

For local management, you can use a computer with terminal emulation software configured to the following parameters:

- VT100 terminal emulation
- 9600 bps
- No parity, 8 data bits, 1 stop bit
- No flow control

Connect the male 9-pin end of the console cable to the console port of the ES-3024 switch. Connect the female end to a serial port (COM1, COM2 or other COM port) of your computer.

3.1.2 Ethernet Ports

The ES-3024 has 10/100Mbps auto-negotiating, auto-crossover Ethernet ports. In 10/100Mbps Fast Ethernet, the speed can be 10Mbps or 100Mbps and the duplex mode can be half duplex or full duplex (100 Mbps only).

When auto-negotiation is turned on, an Ethernet port on the ES-3024 switch negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer Ethernet port does not support auto-negotiation or turns off this feature, the ES-3024 switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the ES-3024 switch's auto-negotiation is turned off, an Ethernet port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer Ethernet port are the same in order to connect.

Default Ethernet Negotiation Settings

The factory default negotiation settings for the Ethernet ports on the ES-3024 switch are:

- Speed: Auto
- Duplex: Auto
- Flow control: On
- Trunking: Disabled

Auto-crossover

All ports are auto-crossover, that is auto-MDIX ports (Media Dependent Interface Crossover), so you may use either a straight through Ethernet cable or crossover Ethernet cable for all Ethernet port connections. Auto-crossover ports automatically sense whether they need to function as crossover or straight ports, so crossover cables can connect both computers and switches/hubs.

3.2 Uplink Modules

LEDs in the (optional) uplink modules are described in the corresponding module manual.

3.2.1 Installing Modules

You can install one stacking module and up to two (optional) uplink modules separately to meet the needs of your network. See your module manual for module specifications.

Modules are NOT hot swappable!

Follow these steps to install the optional modules.

Step 1. Make sure the power cord is not connected to the switch.

Step 2. Loosen the thumbscrews from the cover plate and remove the cover plate from the optional slot. Do not discard the cover plate. You can put the cover plate back on if you remove the new module.

Figure 3-2 Loosening the Screws and Removing the Cover Plate

Step 3. You should wear an anti-static wrist strap or touch any grounded or metal objects to discharge any bodily static electricity before you continue.

Step 4. Remove the optional module from its protective anti-static packaging. Avoid touching the onboard circuit components by holding it by the edge.

Step 5. Insert the optional module into an available expansion slot on the switch. Press it firmly until the optional module snaps into place.

Step 6. Secure it to the switch with the retaining screws.

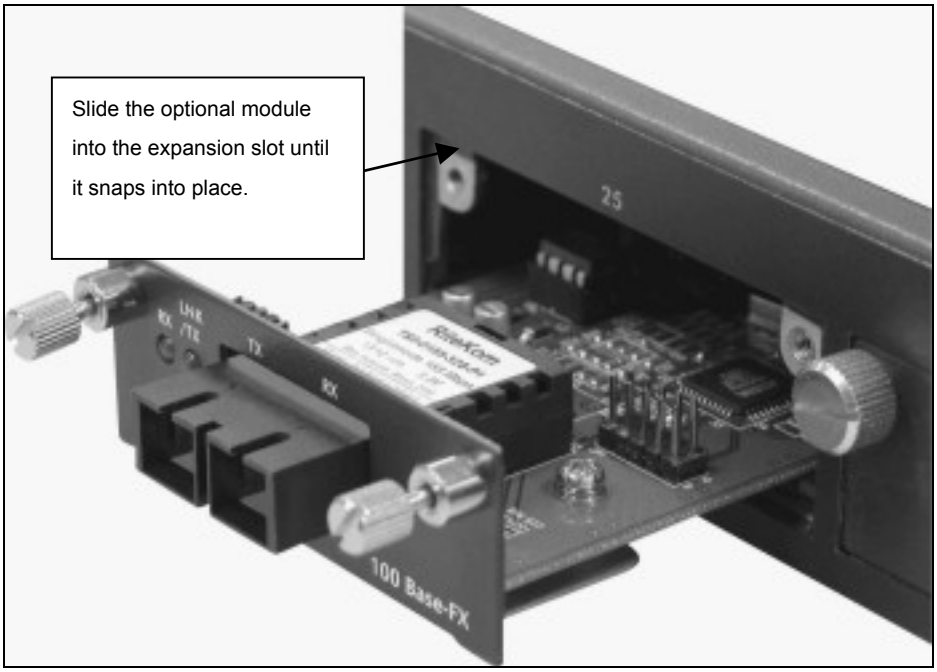

Figure 3-3 Inserting An Example Module[1]

Never force, bend or twist the optional modules into the expansion slots.

Step 7. See section *3.3.1* for instructions on connecting the power. The switch automatically detects the installed optional module. Connect any necessary network cables to the optional module and check the LEDs to verify that it is functioning properly.

[1] This is an example module only!

3.3 Rear Panel

The following figure shows the rear panel of the ES-3024. The rear panel contains the slot for the stacking module and the power receptacle. See *section 3.2.1* for information on inserting and removing modules.

Figure 3-4 ES-3024 Rear Panel

3.3.1 Power Connector

Make sure you are using the correct power source as shown on the panel.

To connect the power to the unit, insert the female end of power cord to the power receptacle on the rear panel. Connect the other end of the supplied power cord to a 100~240VAC/1.5A power outlet. Make sure that no objects obstruct the airflow of the fans (located on the side of the unit).

3.4 Front Panel LEDs

After you connect the power to the switch, view the LEDs to ensure proper functioning of the switch and as an aid in troubleshooting. The front panel LEDs are as follows.

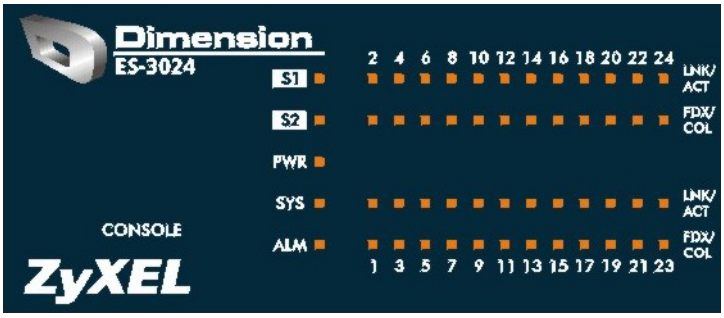

Figure 3-5 Front Panel LEDs

The following table describes the LED indicators on the front panel of an ES-3024 switch.

Table 3-2 ES-3024 Switches: LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
S1	Green	Blinking	The system is transmitting/receiving through the stacking port.
S2		ON	The link through the stacking port is up.
		OFF	The link through the stacking port is down.
PWR	Green	ON	The system is turned on.
		OFF	The system is off.

Table 3-2 ES-3024 Switches: LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
SYS	Green	Blinking	The system is rebooting and performing self-diagnostic tests.
		ON	The system is on and functioning properly.
		OFF	The power is off or the system is not ready/malfunctioning.
ALM	Red	ON	There is a hardware failure.
		OFF	The system is functioning normally.
LNK/ACT (Ethernet ports)	Green	Blinking	The system is transmitting/receiving to/from a 10 Mbps Ethernet network.
		ON	The link to a 10 Mbps Ethernet network is up.
		OFF	The link to a 10 Mbps Ethernet network is down.
	Yellow	Blinking	The system is transmitting/receiving to/from a 100 Mbps Ethernet network.
		ON	The link to a 100 Mbps Ethernet network is up.
		OFF	The link to a 100 Mbps Ethernet network is down.
FDX/COL (Ethernet ports)	Yellow	Blinking	The Ethernet port is negotiating in half-duplex mode and collisions are occurring; the more collisions that occur the faster the LED blinks.
		ON	The Ethernet port is negotiating in full-duplex mode.
		OFF	The Ethernet port is negotiating in half-duplex mode and no collisions are occurring.

3.5 Stacking Scenario Examples

Use Ethernet cables when stacking the switches. See the following figures for example stacking scenarios using the stacking module. The switches must form a closed ring in all scenarios.

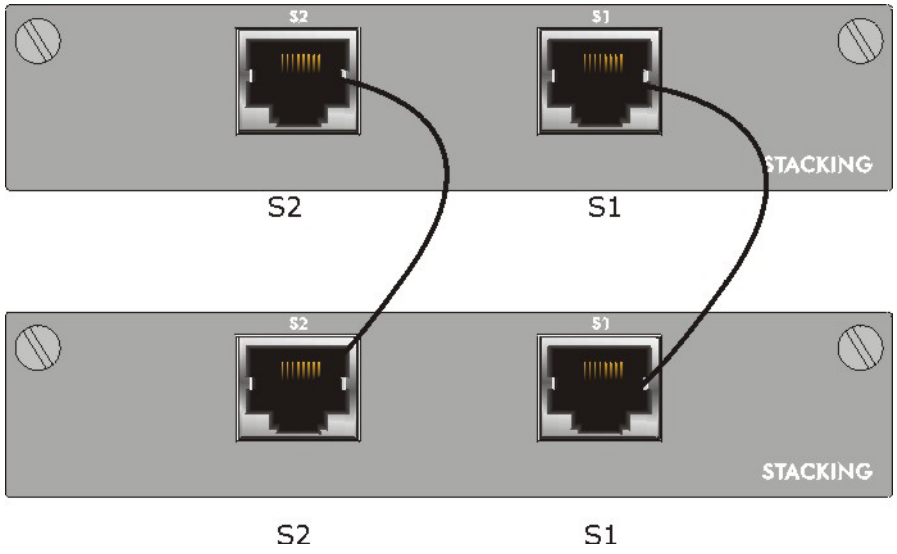

Figure 3-6 Stacking Example 1

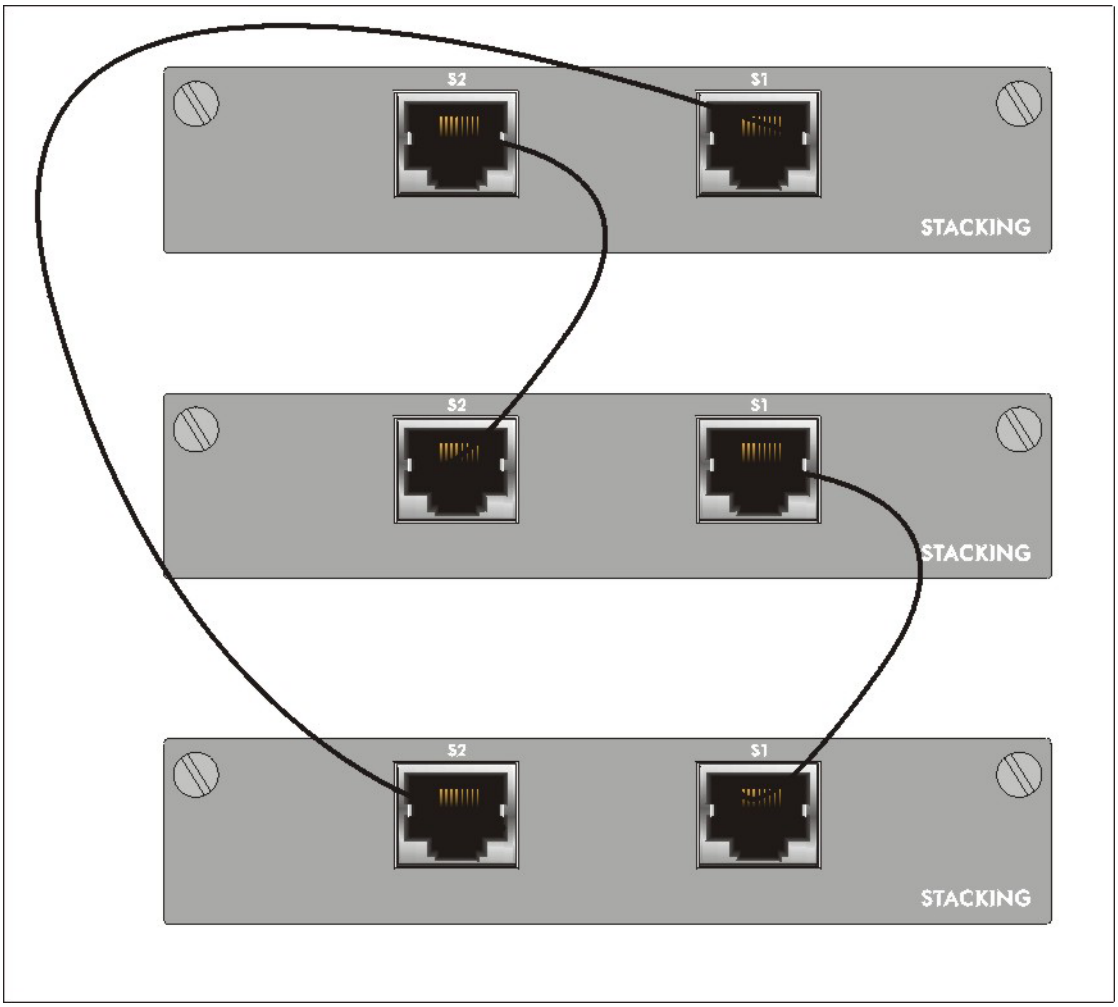

Figure 3-7 Stacking Example 2

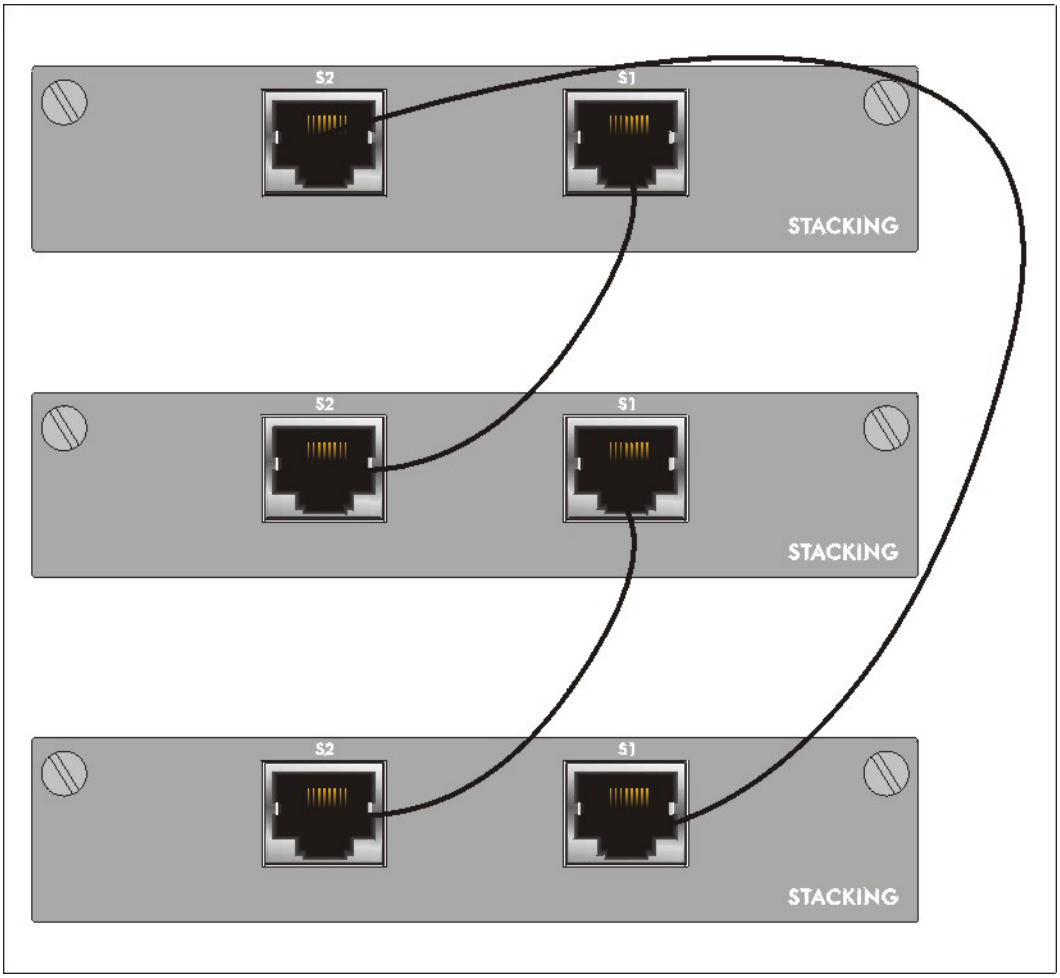

Figure 3-8 Stacking Example 3

See the *Commands Introduction* and *Commonly Used Commands* chapters for information on configuring the stacking modules (as well as other ports) using line commands.

3.6 Uplink Scenario Example

Use Ethernet cables when daisy-chaining/uplinking the switches. See the following figure for an example uplink connection using the stacking module. You must uplink to a Gigabit switch when uplinking using the stacking module. Uplink scenarios using an uplink module depend on the uplink module you use.

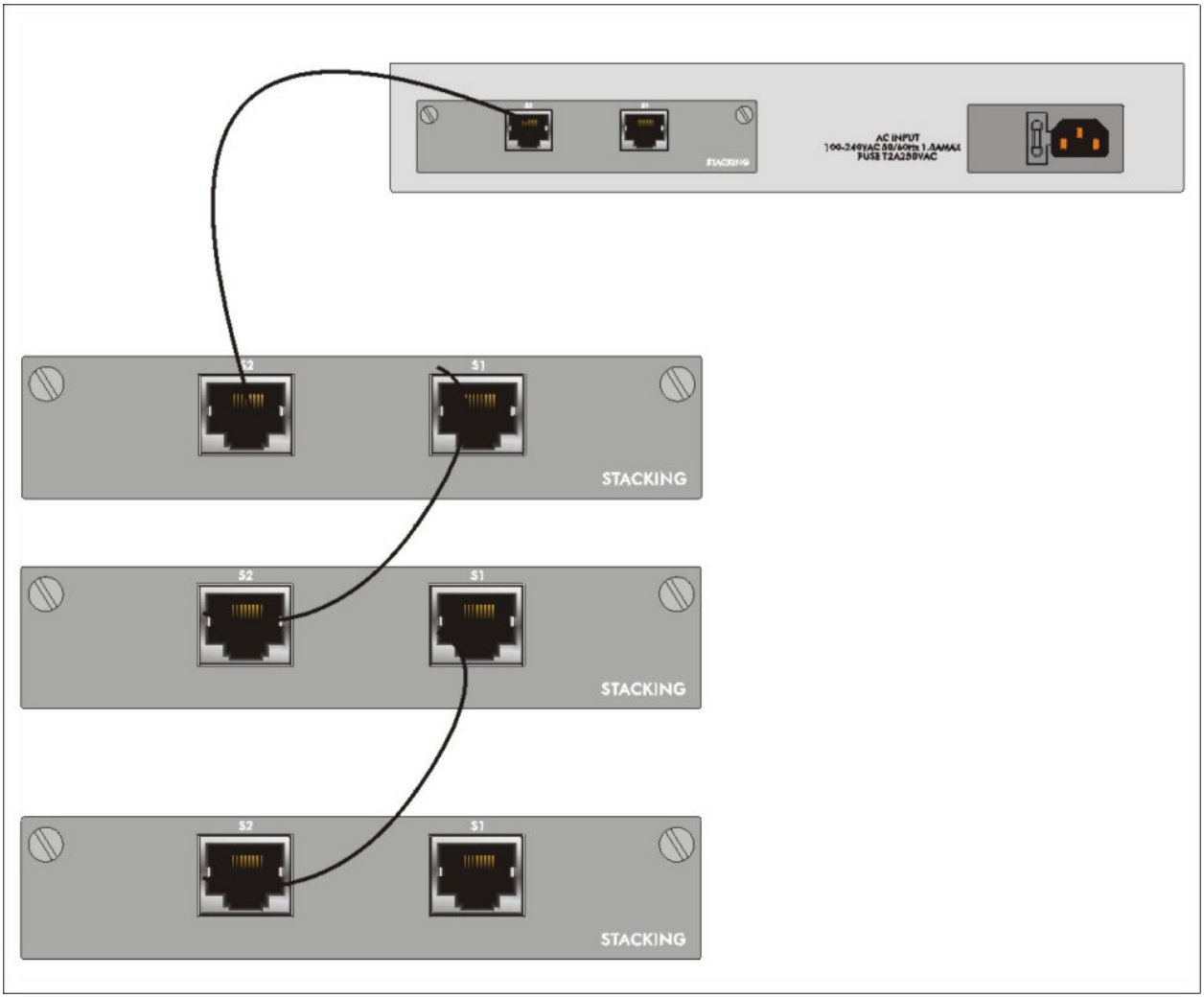

Figure 3-9 Uplink Example

3.7 Configuring the ES-3024

You may use the embedded web configurator or command line interface to configure the ES-3024. If you're using the web configurator, you need Internet Explorer 5.5 and later or Netscape Navigator 6 and later.

You can access the command line interface using a terminal emulation program on a computer connected to the switch console port (see *section 3.1.1*) or access the switch via an Ethernet port using Telnet.

When using the command line interface, you can only save STP, 802.1q and 802.1d configurations using the "config save" command. All other configurations done using the command line interface are effective only until you restart the switch.

The next part of this guide discusses configuring the ES-3024 using the web configurator.

Part III

Getting Started

This part introduces you to the ES-3024 web configurator and how to use it to configure the Getting Started menus.

Chapter 4
Introducing the Web Configurator

This section introduces the configuration and functions of the Web Configurator.

4.1 Introduction

The embedded web configurator allows you to manage the switch from anywhere through a standard browser such as Microsoft Internet Explorer or Netscape Navigator.

Use Internet Explorer 5.5 and later or Netscape Navigator 6 and later versions.

4.2 System Login

A local console port connection locks out all other connections. Log out from the console port connection before logging in with the Web Configurator.

Step 1. Start Internet Explorer or Netscape Communicator web browser.

Step 2. Type http:// and the IP address of the switch (for example, the default is 192.168.1.1) in the Location or Address field. Press **Enter**.

Figure 4-1 Web Configurator - Login

Step 3. The **Password** screen appears. The default username is **admin** and associated default password is **1234**.

Step 4. Click **Login**. The **Home** screen of the web configurator displays.

4.2.1 Change Your Password

This screen prompts you to change your password if it is still set to the default. It is highly recommended you change the password.

Figure 4-2 Change Password Screen

4.3 Switch Lockout

You are locked out from managing the switch if another administrator is currently logged in. You must wait until he/she has logged out before you can log in.

Moreover, you could lock yourself (and all others) out from the switch by:

1. Deleting the management VLAN (default is VLAN 1).
2. Deleting all port-based VLANs with the CPU port as a member. The "CPU port" is the management port of the switch.
3. Filtering all traffic to the CPU port.
4. Disabling all ports.
5. Assigning minimum bandwidth to the CPU port. If you limit bandwidth to the CPU port, you may find that the switch performs sluggishly or not at all.

Be careful not to lock yourself and others out of the switch.

4.4 Resetting the Switch

If you lock yourself (and others) from the switch or forget the ES-3024 password, you will need to reload the factory-default configuration file.

Uploading the factory-default configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all previous configurations and the speed of the console port will be reset to the default of 9600bps with 8 data bit, no parity, one stop bit and flow control set to none. The password will also be reset to "1234" and the IP address to 192.168.1.1.

To upload the configuration file, do the following:

Step 1. Connect to the console port using a computer with terminal emulation software. See the *Hardware Connections* chapter for details.

Step 2. Disconnect and reconnect the switch's power to begin a session. When you reconnect the switch's power, you will see the initial screen.

Step 3. When you see the message "Press any key to enter Debug Mode within 3 seconds" press any key to enter debug mode.

Step 4. Type `atlc` after the `Enter Debug Mode` message.

Step 5. Wait for the `Starting XMODEM upload` message before activating XMODEM upload on your terminal.

Step 6. After a successful firmware upload, type `atgo` to restart the switch.

The switch is now reinitialized with a default configuration file including the default password of "1234".

4.5 Home Screen

The home screen consists of a navigation panel and a main panel.

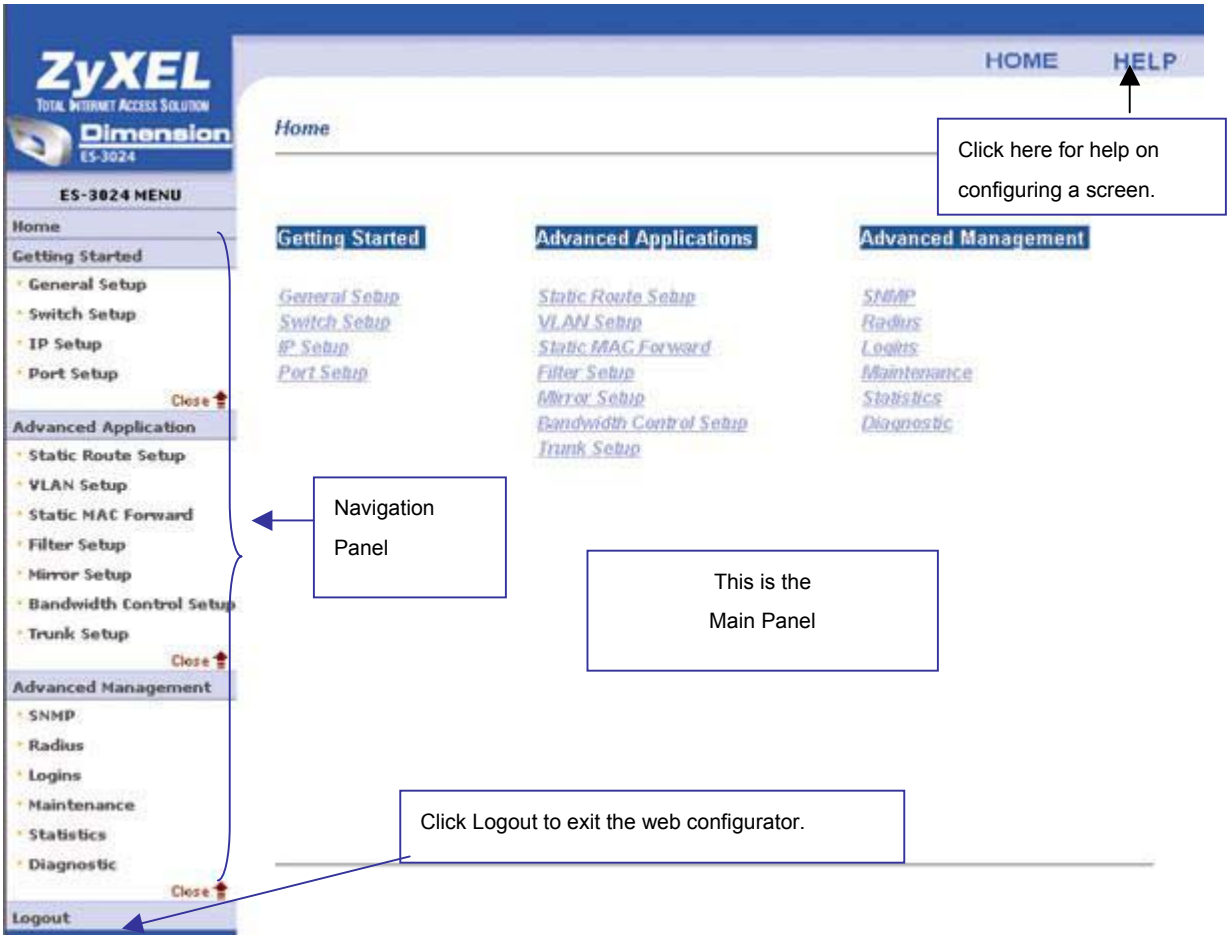

Figure 4-3 ES-3024 Home Screen

Table 4-1 Navigation Panel Links

LABEL	DESCRIPTION
Getting Started	
General Setup	This link takes you to a screen where you can configure general identification information about the switch.
Switch Setup	This link takes you to a screen where you can set up global switch parameters such as VLAN type, MAC address learning, IGMP snooping, GARP, priority queues, STP, broadcast storm control, LACP trunking and 802.1X authentication.
IP Setup	This link takes you to a screen where you can configure the IP address, subnet mask (necessary for switch management) and DNS (domain name server).
Port Setup	This link takes you to screens where you can configure settings for individual switch ports.
Advanced Applications	
Static Route Setup	This link takes you to screens where you can configure static routes. A static route defines how the ES-3024 should forward traffic by configuring the TCP/IP parameters manually.
VLAN Setup	This link takes you to screens where you can configure port-based or 802.1Q VLAN (depending on what you configured in the **Switch Setup** menu).
Static MAC Forward	This link takes you to screens where you can configure static MAC addresses for a port. These static MAC addresses do not age out.
Filter Setup	This link takes you to screens where you can filter traffic going from one port or ports to another port or ports.
Mirror Setup	This link takes you to screens where you can copy traffic from one port or ports to another port in order that you can examine the traffic from the first port without interference
Bandwidth Control Setup	This link takes you to screens where you can cap the maximum bandwidth allowed from specified source(s) to specified destination(s).
Trunk Setup	This link takes you to a screen where you can logically aggregate physical links to form one logical, higher-bandwidth link.
Advanced Management	
SNMP	This link takes you to a screen where you can configure SNMP (Simple Network Management Protocol) for network management and monitoring.
RADIUS	This link takes you to a screen where you can configure RADIUS (Remote Authentication Dial-In User Service), a protocol for user authentication that allows you to use an external server to validate an unlimited number of users.
Logins	This link takes you to a screen where you can change your password and configure passwords for up to four administrators. Only one administrator can be active at any one time.
Maintenance	This link takes you to screens where you can set UNIX syslog parameters, time and date and remote management as well as perform firmware and configuration file maintenance.
Statistics	This link takes you to screens where you can view switch statistical information.
Diagnostic	This link takes you to screens where you can view system logs and test port(s).
Logout	Click here to exit the web configurator. You have to log in with your password again after you log out. This is recommended after you finish a management session both for security reasons and so as you don't lock out other switch administrators.

4.5.1 Help

The web configurator's online help has descriptions of individual screens and some supplementary information.

Click the **HELP** link from the home screen to view the online help's home screen summary menu.

Click the **HELP** link from a web configurator screen other than the home screen to view an online help description of that screen.

4.6 Screen Overview

The following table lists the various web configurator screens.

Table 4-2 Web Configurator Screen Overview

GETTING STARTED	ADVANCED APPLICATIONS	ADVANCED MANAGEMENT
General Setup	Static Route Setup	SNMP
Switch Setup	Edit Static Route	RADIUS
IP Setup	VLAN Setup	Logins
Port Setup	Edit VLAN Static Entry	Maintenance
Edit Port Setup	Static MAC Forward	Remote Management
	Edit Static MAC Forward	Edit Secured Clients
	Filter Setup	Upgrade Firmware
	Edit Filter Setup	Restore Configuration
	Mirror Setup	Backup Configuration
	Edit Mirror Setup	Statistics
	Bandwidth Control Setup	Diagnostic General
	Edit Bandwidth Control Setup	Diagnostic Ethernet Port
	Trunk Setup	

The next chapters discuss the Getting Started screens.

Chapter 5
General, Switch and IP Setup

This chapter describes how to configure the aforementioned screens.

5.1 Introduction

The **General Setup** screen allows you to configure general switch identification information. The **Switch Setup** screen allows you to set up and configure global switch features. The **IP Setup** screen allows you to configure an IP address, subnet mask and DNS (domain name server) for the switch for management purposes.

5.2 General Setup

Click **General Setup** in the navigation panel to open this screen.

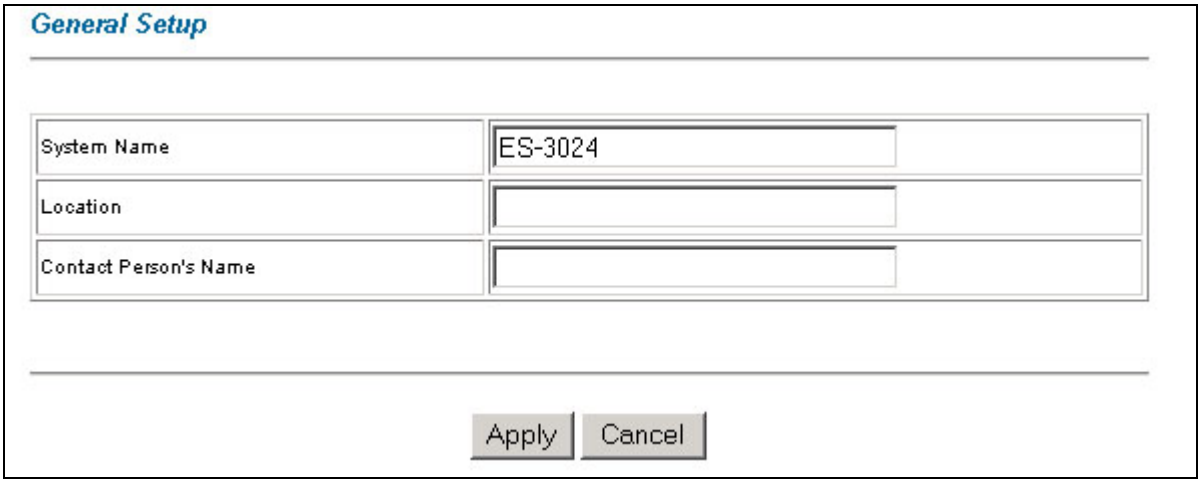

Figure 5-1 General Setup

Table 5-1 General Setup

LABEL	DESCRIPTION
System Name	Choose a descriptive name for identification purposes. This name can be up to 30 alphanumeric characters long.
Location	Enter the geographic location (up to 30 characters) of your switch.
Contact Person's Name	Enter the name (up to 30 characters) of the person in charge of this switch.
Click **Apply** to save your changes back to the switch. Click **Cancel** to begin configuring this screen afresh.	

5.3 IGMP Snooping

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender to 1 recipient) or Broadcast (1 sender to everybody on the network). Multicast delivers IP packets to just a group of hosts on the network.

IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a multicast group - it is not used to carry user data. Refer to *RFC 1112* and *RFC 2236* for information on IGMP versions 1 and 2 respectively.

A layer-2 switch can passively snoop on IGMP Query, Report and Leave (IGMP version 2) packets transferred between IP multicast routers/switches and IP multicast hosts to learn the IP multicast group membership. It checks IGMP packets passing through it, picks out the group registration information, and configures multicasting accordingly.

Without IGMP snooping, multicast traffic is treated in the same manner as broadcast traffic, that is, it is forwarded to all ports. With IGMP snooping, group multicast traffic is only forwarded to ports that are members of that group. IGMP Snooping generates no additional network traffic, allowing you to significantly reduce multicast traffic passing through your switch.

5.4 Introduction to VLANs

A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Stations on a logical network belong to one group. A station can belong to more than one group. With VLAN, a station cannot directly talk to or hear from stations that are not in the same group(s); the traffic must first go through a router.

In MTU (Multi-Tenant Unit) applications, VLAN is vital in providing isolation and security among the subscribers. When properly configured, VLAN prevents one subscriber from accessing the network resources of another on the same LAN, thus a user will not see the printers and hard disks of another user in the same building.

VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

Note that VLAN is unidirectional; it only governs outgoing traffic.

See the *VLAN Setup* chapter for information on port-based and 802.1Q tagged VLANs.

5.5 Introduction to Spanning Tree Protocol (STP)

STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a switch to interact with other STP-compliant switches in your network to ensure that only one route exists between any two stations on the network.

5.5.1 STP Terminology

The root bridge is the base of the spanning tree; it is the bridge with the lowest identifier value (MAC address).

Path cost is the cost of transmitting a frame onto a LAN through that port. It is assigned according to the speed of the link to which a port is attached. The slower the media, the higher the cost - see the next table.

Table 5-2 STP Path Costs

	LINK SPEED	RECOMMENDED VALUE	RECOMMENDED RANGE	ALLOWED RANGE
Path Cost	4Mbps	250	100 to 1000	1 to 65535
Path Cost	10Mbps	100	50 to 600	1 to 65535
Path Cost	16Mbps	62	40 to 400	1 to 65535
Path Cost	100Mbps	19	10 to 60	1 to 65535
Path Cost	1Gbps	4	3 to 10	1 to 65535
Path Cost	10Gbps	2	1 to 5	1 to 65535

On each bridge, the root port is the port through which this bridge communicates with the root. It is the port on this switch with the lowest path cost to the root (the root path cost). If there is no root port, then this switch has been accepted as the root bridge of the spanning tree network.

For each LAN segment, a designated bridge is selected. This bridge has the lowest cost to the root among the bridges connected to the LAN.

5.5.2 How STP Works

After a bridge determines the lowest cost-spanning tree with STP, it enables the root port and the ports that are the designated ports for connected LANs, and disables all other ports that participate in STP. Network packets are therefore only forwarded between enabled ports, eliminating any possible network loops.

STP-aware switches exchange Bridge Protocol Data Units (BPDUs) periodically. When the bridged LAN topology changes, a new spanning tree is constructed.

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (Max Age), the bridge assumes that the link to the root bridge is down. This bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology.

5.5.3 STP Port States

STP assigns five port states (see next table) to eliminate packet looping. A bridge port is not allowed to go directly from blocking state to forwarding state so as to eliminate transient loops.

Table 5-3 STP Port States

PORT STATE	DESCRIPTION
Disabled	STP is disabled (default).
Blocking	Only configuration and management BPDUs are received and processed.
Listening	All BPDUs are received and processed.

Table 5-3 STP Port States

PORT STATE	DESCRIPTION
Learning	All BPDUs are received and processed. Information frames are submitted to the learning process but not forwarded.
Forwarding	All BPDUs are received and processed. All information frames are received and forwarded.

5.6 Dynamic Link Aggregation

The ES-3024 supports the link aggregation IEEE802.3ad standard. This standard describes the Link Aggregate Control Protocol (LACP), which is a protocol that dynamically creates and manages trunk groups.

When you enable LACP link aggregation on a port, the port can automatically negotiate with the ports at the remote end of a link to establish trunk groups. LACP also allows port redundancy, that is, if an operational port fails, then one of the "standby" ports become operational without user intervention

Please note that:

- You must connect all ports point-to-point to the same Ethernet switch and configure the ports for LACP trunking.
- LACP only works on full-duplex links.
- All ports in the same trunk group must have the same media type, speed, duplex mode and flow control settings.
- Configure trunk groups or LACP before you connect the Ethernet switch to avoid causing network topology loops.

5.7 802.1X Authentication

See the ***Port Setup*** chapter for more information on 802.1x authentication.

5.8 Switch Setup Screen

Click **Switch Setup** in the navigation panel to open the **Switch Setup** screen. The **VLAN Setup** screen changes depending on whether you choose **802.1Q VLAN Type** or **Port Based VLAN Type** in this screen.

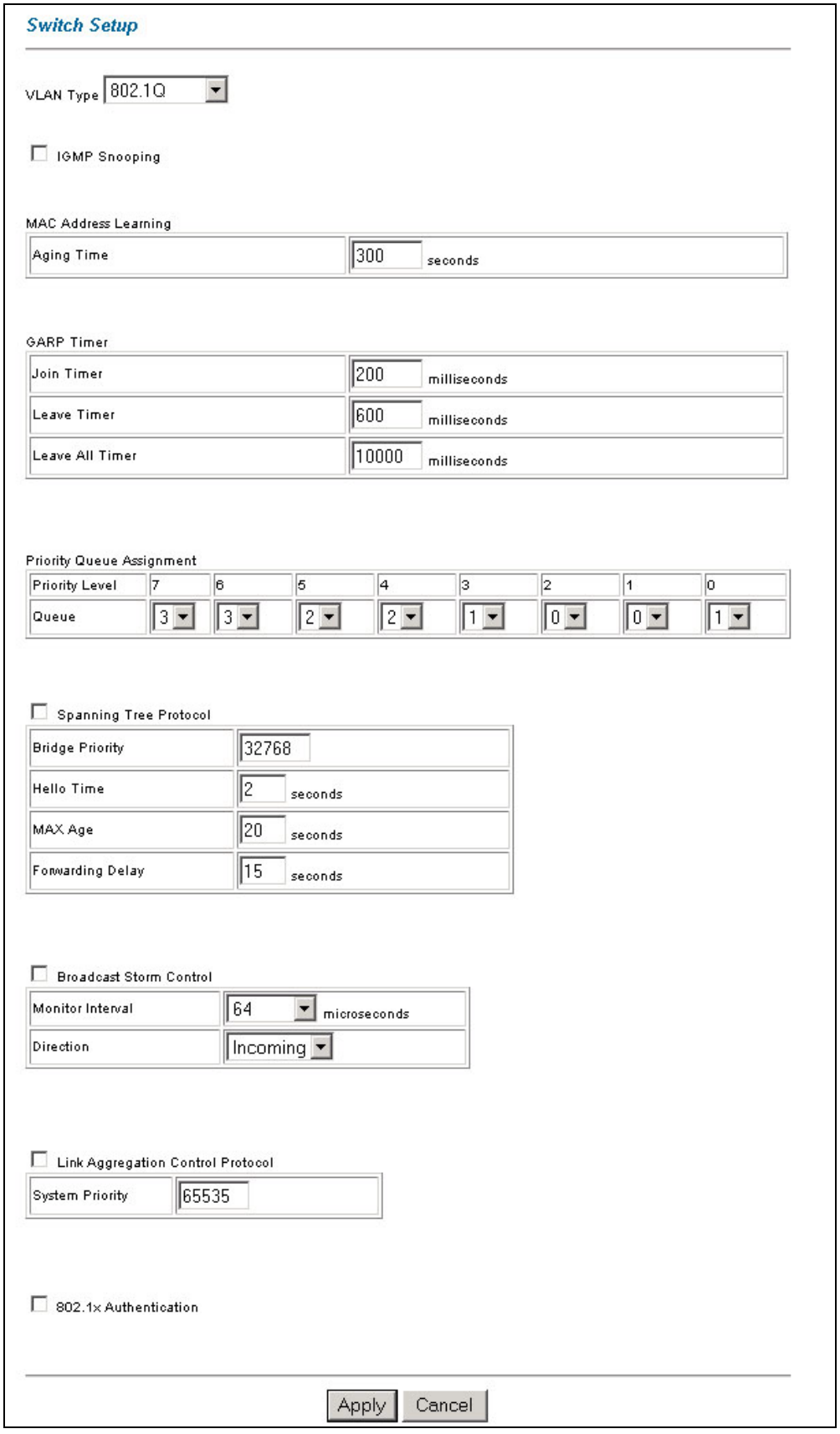

Figure 5-2 Switch Setup

Table 5-4 Switch Setup

LABEL	DESCRIPTION	EXAMPLE
VLAN Type	Choose **802.1Q** or **Port Based** from the drop-down list box. The **VLAN Setup** screen changes depending on whether you choose **802.1Q VLAN Type** or **Port Based VLAN Type** in this screen. See *section 5.4* and the *VLAN Setup* chapter for more information on VLANs.	802.1Q
IGMP Snooping	Select the checkbox to enable IGMP snooping and have group multicast traffic only forwarded to ports that are members of that group, significantly reducing multicast traffic passing through your switch. See *section 5.3* for more information on IGMP snooping.	
MAC Address Learning	MAC address learning reduces outgoing traffic broadcasts. For MAC address learning to occur on a port, the port must be active.	
Aging Time	Enter a time from 0 to 1700 seconds. This is how long all dynamically learned MAC addresses remain in the MAC address table before they age out (and must be relearned).	300
GARP Timer: Switches join VLANs by making a declaration. A declaration is made by issuing a **Join** message using GARP. Declarations are withdrawn by issuing a **Leave** message. A **Leave All** message terminates all registrations. GARP timers set declaration timeout values. See the chapter on VLAN setup for more background information.		
Join Timer	Join Timer sets the duration of the Join Period timer for GVRP in milliseconds. Each port has a Join Period timer. The allowed Join Time range is between 100 and 65535 milliseconds; the default is 200 milliseconds. See the chapter on VLAN setup for more background information.	200 milliseconds (default)
Leave Timer	Leave Timer sets the duration of the Leave Period timer for GVRP in milliseconds. Each port has a single Leave Period timer. Leave Time must be two times larger than Join Timer; the default is 600 milliseconds.	600 milliseconds (default)
Leave All Timer	Leave All Timer sets the duration of the Leave All Period timer for GVRP in milliseconds. Each port has a single Leave All Period timer. Leave All Timer must be larger than Leave Timer; the default is 1000 milliseconds.	1000 milliseconds (default)
Priority Queue Assignment: IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Frames without an explicit priority tag are given the default priority of the ingress port. Use the next two fields to configure the priority level-to-physical queue mapping. The switch has 4 physical queues that you can map to the 8 priority levels. On the switch, traffic assigned to higher index queues gets through faster while traffic in lower index queues is dropped if the network is congested.		
Priority Level (The following descriptions are based on the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p).		
Priority 7	Typically used for network control traffic such as router configuration messages.	
Priority 6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).	
Priority 5	Typically used for video that consumes high bandwidth and is sensitive to jitter.	

Table 5-4 Switch Setup

LABEL	DESCRIPTION	EXAMPLE
Priority 4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.	
Priority 3	Typically used for “excellent effort” or better than best effort and would include important business traffic that can tolerate some delay.	
Priority 2	This is for “spare bandwidth”.	
Priority 1	This is typically used for non-critical “background” traffic such as bulk transfers that are allowed but that should not affect other applications and users.	
Priority 0	Typically used for best-effort traffic.	
Queue	Select from Queue 0 (for lower priority traffic) to Queue 3 (for higher priority traffic) from the drop-down list boxes to map a queue for each traffic type.	
Spanning Tree Protocol: Use STP to detect and disable network loops and provide backup links between switches, bridges or routers. Select Spanning Tree Protocol to enable STP on the switch. After configuring switch STP in this screen, you must configure STP information for each port in the **Port Setup** screen.		
Bridge Priority	Bridge priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch. The allowed range is 0 to 65535. The lower the numeric value you assign, the higher the priority for this bridge. Bridge Priority determines the root bridge, which in turn determines Hello Time, Max Age and Forwarding Delay.	32768 (default)
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.	2 (default)
Max Age	This is the maximum time (in seconds) a switch can wait without receiving a BPDU before attempting to reconfigure. All switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the switch ports attached to the network. The allowed range is 6 to 40 seconds.	20 (default)
Forwarding Delay	This is the maximum time (in seconds) a switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds.	15 (default)
Broadcast Storm Control	Use this field to limit the number of broadcast frames that can be stored in the switch buffer or sent out from the switch. Broadcast frames that arrive when the buffer is full are discarded. Enable **Broadcast Storm Control** to reduce broadcast traffic coming into your network.	

Table 5-4 Switch Setup

LABEL	DESCRIPTION	EXAMPLE
Monitor Interval	When the **Monitor Interval** time period expires, each port begins counting broadcast frames allowed in its buffers anew. Select a time period from **64**, **1024**, **8000**, **256000** microseconds from the drop-down list box.	
Direction	Choose to monitor broadcast packets coming into the switch (**Incoming**) or going out of the switch (**Outgoing**).	
Link Aggregation Control Protocol	Select this checkbox to enable Link Aggregation Control Protocol (LACP). See *the Trunk Setup chapter* for more information on LACP.	
System Priority	LACP system priority is a number between 1 and 65,355. The switch with the lowest system priority (and lowest port number if system priority is the same) becomes the LACP "server". The LACP "server" controls the operation of LACP setup. Enter a number to set the priority of an active port using Link Aggregate Control Protocol (LACP). The smaller the number, the higher the priority level.	65535
802.1x Authentication	Select this checkbox to permit 802.1x authentication on the switch. You must first allow 802.1x authentication on the switch before configuring it on each port.	
Click **Apply** to save your changes back to the switch or click **Cancel** to begin configuring this screen afresh.		

5.9 IP Setup

The switch needs an IP address for it to be managed over the network. The factory default IP address is 192.168.1.1. The subnet mask specifies the network number portion of an IP address. The factory default subnet mask is 255.255.255.0. The default gateway specifies the IP address of the default gateway (next hop) for outgoing traffic. 0.0.0.0 means no default gateway is specified.

Click **IP Setup** in the navigation panel to open this screen.

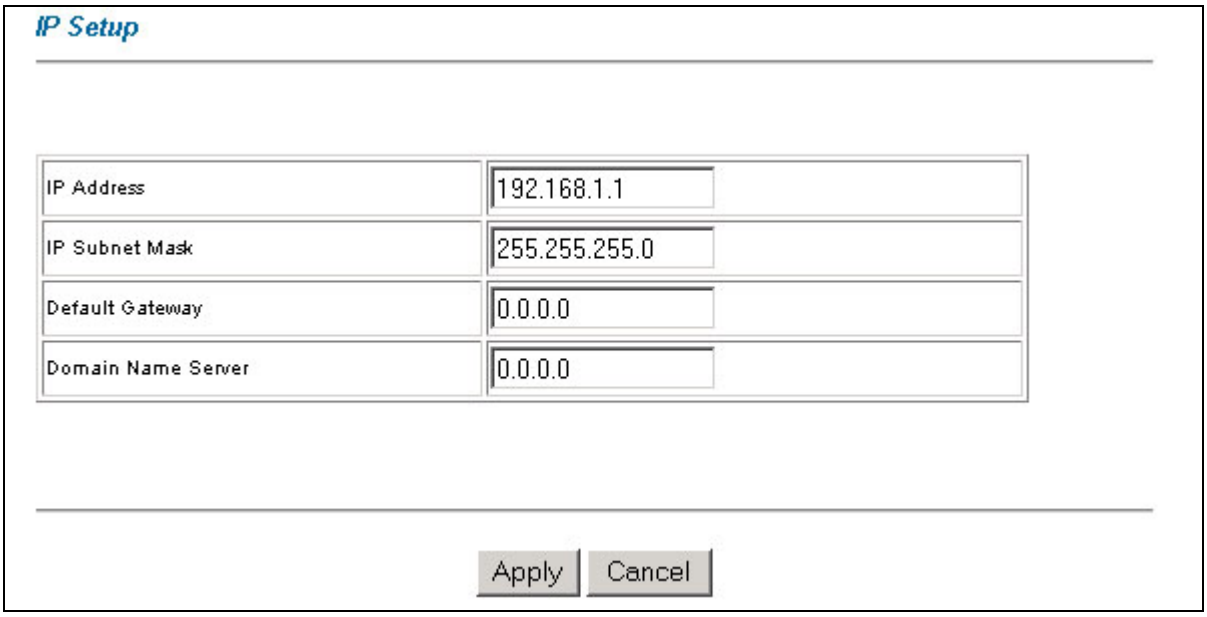

Figure 5-3 IP Setup

Table 5-5 IP Setup

LABEL	DESCRIPTION
IP Address	Enter the IP address of your switch in dotted decimal notation for example 192.168.1.1.
IP Subnet Mask	Enter the IP subnet mask of your switch in dotted decimal notation for example 255.255.255.0.
Default Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.1.254.
Domain Name Server	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. Enter a domain name server IP address in order to be able to use a domain name instead of an IP address in the **Time and Date** screen.
Click **Apply** to save your changes back to the switch. Click **Cancel** to begin configuring this screen afresh.	

Chapter 6
Port Setup

This chapter explains how to configure individual ports on the ES-3024.

6.1 Introduction

Click **Port Setup** from the navigation panel to enter the port configuration summary screen. You may configure any of the 26 Ethernet ports (ports 25 and 26 are uplink ports) by clicking its index number.

Port Setup

Port	Active	Name	Type	Speed	Duplex
Port 1	Yes	none	10/100M	Auto	N/A
Port 2	Yes	none	10/100M	Auto	N/A
Port 3	Yes	none	10/100M	Auto	N/A
Port 4	Yes	none	10/100M	Auto	N/A
Port 5	Yes	none	10/100M	Auto	N/A
Port 6	Yes	none	10/100M	Auto	N/A
Port 7	Yes	none	10/100M	Auto	N/A
Port 8	Yes	none	10/100M	Auto	N/A
Port 9	Yes	none	10/100M	Auto	N/A
Port 10	Yes	none	10/100M	Auto	N/A
Port 11	Yes	none	10/100M	Auto	N/A
Port 12	Yes	none	10/100M	Auto	N/A
Port 13	Yes	none	10/100M	Auto	N/A
Port 14	Yes	none	10/100M	Auto	N/A
Port 15	Yes	none	10/100M	Auto	N/A
Port 16	Yes	none	10/100M	Auto	N/A
Port 17	Yes	none	10/100M	Auto	N/A
Port 18	Yes	none	10/100M	Auto	N/A
Port 19	Yes	none	10/100M	Auto	N/A
Port 20	Yes	none	10/100M	Auto	N/A
Port 21	Yes	none	10/100M	Auto	N/A
Port 22	Yes	none	10/100M	Auto	N/A
Port 23	Yes	none	10/100M	Auto	N/A
Port 24	Yes	none	10/100M	Auto	N/A
Port 25	Yes	none	Empty	N/A	N/A
Port 26	Yes	none	Empty	N/A	N/A

Figure 6-1 Port Setup Summary Screen

Table 6-1 Port Setup Summary Screen

LABEL	DESCRIPTION
Port	This is the port index number. Click a port link to configure that port.
Active	This field shows whether the port is turned on (**Yes**) or not (**No**). The factory default for all ports is disabled. A port must be enabled for data transmission to occur.
Name	This field shows the name that identifies this port.
Type	This field displays **10/100M** for an Ethernet/Fast Ethernet connection and **Empty** if no uplink module is inserted in the slot. If an uplink module is present, then its type is displayed here.
Speed	This field displays the configured speed or **Auto** of the Ethernet port. **Auto** means the switch automatically finds the speed of the attached switch.
Duplex	This field displays the Ethernet duplex mode, that is full-duplex (**Full**) or half-duplex (**Half**) or **N/A** when **Auto** is selected as the speed.

6.2 IEEE 802.1x

IEEE 802.1x is an extended authentication protocol[1] that allows support of RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting[2] management on a network RADIUS server.

You must enable 802.1x on the switch (see **Switch Setup** screen) before enabling it on a port.

6.3 Configure 802.1x on a Port

Click a port link in the **Port Setup** summary screen to enter that port's configuration screen.

[1] At the time of writing, only Windows XP of the Microsoft operating systems supports it. See the Microsoft web site for information on other Windows operating system support. For other operating systems, see its documentation. If your operating system does not support 802.1x, then you may need to install 802.1x client software.

[2] Not available at the time of writing.

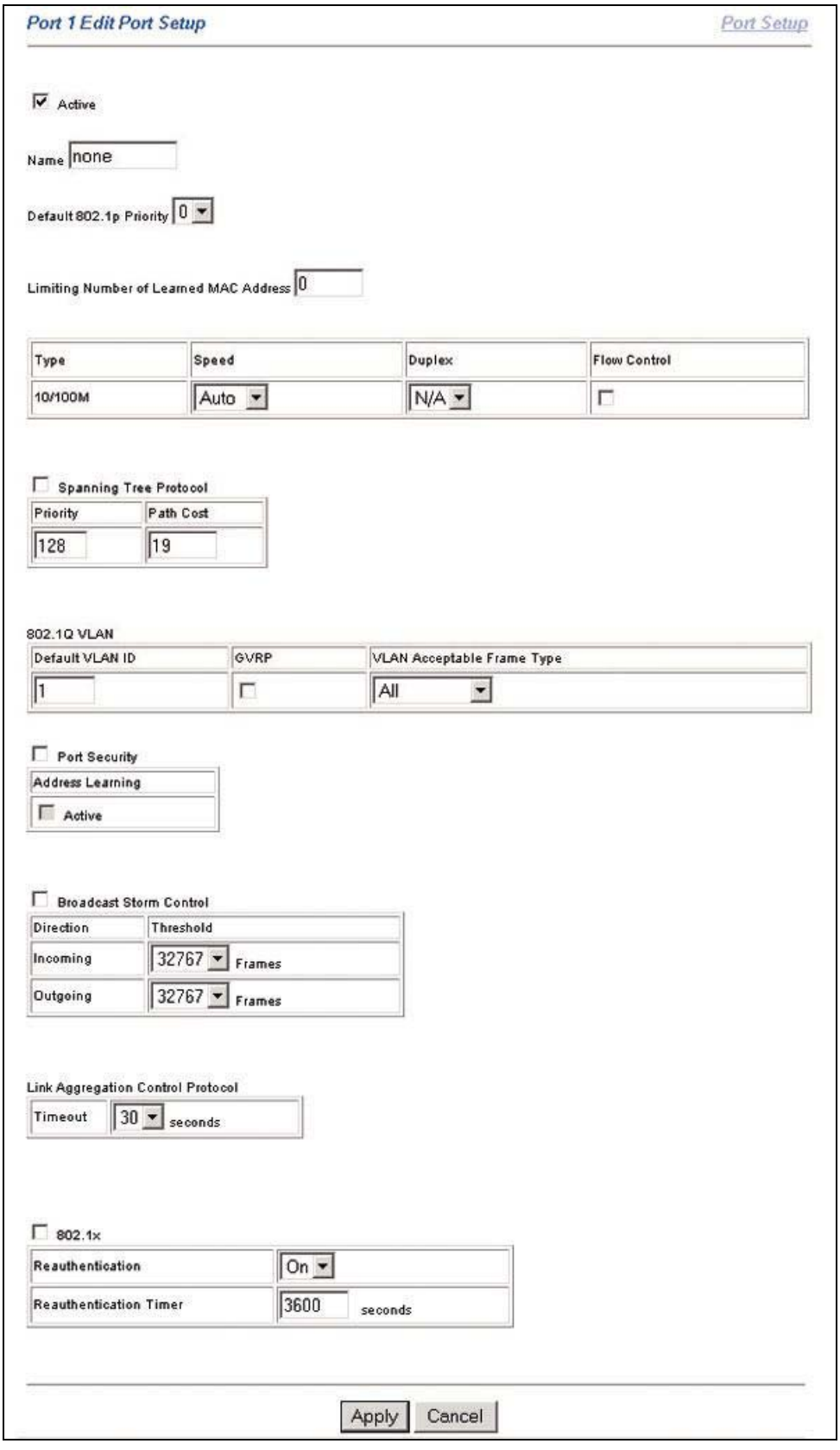

Figure 6-2 Port Edit Screen

Table 6-2 Port Edit Screen

LABEL	DESCRIPTION	EXAMPLE
Active	A port must be enabled for data transmission to occur. Select **Active** to enable the port.	
Name	Choose a descriptive name for port identification purposes.	Joe
Default 802.1P Priority	This priority value is added to incoming frames without a (802.1p) priority queue tag. See **Priority Queue Assignment** in *Table 5-4 Switch Setup* for more information.	0 (default)
Limiting Number of Learned MAC Address	Use this field to limit the number of (dynamic) MAC addresses that may be learned on a port. For example, if you set this field to "5" on port 2, then only the devices with these five learned MAC addresses may access port 2 at any one time. A sixth device would have to wait until one of the five learned MAC addresses aged out. MAC-address aging out time can be set in the **Switch Setup** screen. The valid range is from “0” to “254”. “0” means this feature is disabled, so the switch will learn MAC addresses up to the global limit of 16K.	0
Type	This read-only label displays the type of port you are currently configuring.	10/100M
Speed	Select the speed of the Ethernet connection on this port. **Auto** (auto-negotiation) makes one Ethernet port able to negotiate with a peer automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, an Ethernet port on the switch negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer Ethernet port does not support auto-negotiation or turns off this feature, the switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the switch’s auto-negotiation is turned off, an Ethernet port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer Ethernet port are the same in order to connect.	**Auto**
Duplex	Select a duplex mode from half duplex (**Half**), full duplex (**Full**) or (**N/A**). **N/A** displays when auto-negotiation is turned on, as the Ethernet port on the switch negotiates with the peer automatically to determine the connection speed and duplex mode.	**Full**
Flow Control	A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses. **Flow Control** is used to regulate transmission of signals to match the bandwidth of the receiving port. The ES-3024 uses IEEE802.3x flow control in full duplex mode and backpressure flow control in half duplex mode. IEEE802.3 flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill. Back Pressure flow control is typically used in half duplex mode to send a "collision" signal to the sending port (mimicking a state of packet collision) causing the sending port to temporarily stop sending signals and resend later. Select **Flow Control** to enable it.	

Table 6-2 Port Edit Screen

LABEL	DESCRIPTION	EXAMPLE
Spanning Tree Protocol	Select **Spanning Tree Protocol** to enable. See *section 5.5* for more information.	
Priority	Configure the priority for each port here. Priority decides which port should be disabled when more than one port forms a loop in a switch. Ports with a higher priority numeric value are disabled first. The allowed range is between 0 and 255 and default value is 128.	128 (default)
Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is assigned according to the speed of the bridge. The slower the media, the higher the cost - see *Table 5-2 STP Path Costs* for more information.	100
802.1Q VLAN: These fields are only visible if you chose **802.1Q** In the **VLAN Type** field in the **Switch Setup** screen.		
Default VLAN ID	Default VLAN ID is the PVID, the Port VLAN ID assigned to untagged frames or priority-tagged frames received on this port.	1(default)
GVRP	GVRP (GARP VLAN Registration Protocol) is a registration protocol that defines a way for switches to register necessary VLAN members on ports across the network. Select this check box to enable GVRP and propagate VLANs information beyond the local switch.	
VLAN Acceptable Frame Type	Choose **All** if you want the port to accept both tagged and untagged incoming packets (to that port). Choose **Tagged** if you want the port to accept just tagged incoming packets (to that port). See *section 5.4* for more information on VLANs.	All
Port Security	Port security means that only packets with dynamically learned MAC addresses and/or configured static MAC addresses can pass through this port. The switch can learn up to 16K MAC addresses in total with no limit on individual ports other than the sum cannot exceed 16K. For maximum port security, enable **Port Security**, disable Mac address learning and configure static MAC address(es) for that port. It is not recommended you disable **Port Security** together with MAC address learning as this will result in many broadcasts.	
Address Learning	MAC address learning reduces outgoing broadcast traffic. For MAC address learning to occur on a port, the port must port must have address learning active and the port itself must be active.	
Active	Select **Active** to enable MAC address learning on this port.	

Table 6-2 Port Edit Screen

LABEL	DESCRIPTION	EXAMPLE
Broadcast Storm Control	Enable **Broadcast Storm Control** to reduce broadcast traffic coming into or going out of this port. Broadcast Storm Control includes multicast packets. Use the **Threshold** field to limit the number of broadcast frames that can be: ➢ Stored in a port's buffer or ➢ Sent out from the port. Broadcast frames that arrive within the monitor interval specified in the **Switch Setup** screen but after the buffer is full are discarded.	
Threshold	Select the number of frames allowed in the **Threshold** drop-down list box. If you wish your network to receive or broadcast a lot of broadcast traffic then choose a larger number. To reduce broadcast traffic coming into or going out of your network, choose a smaller number.	**128**
Direction	Select **Incoming** to control how many broadcast frames the port can store in the switch buffer and select **Outgoing** to control how many frames the port will send out.	**incoming**
Link Aggregate Control Protocol	The ES-3024 supports the link aggregation IEEE802.3ad standard. This standard describes the Link Aggregate Control Protocol (LACP), which is a protocol that is used to dynamically create and manage trunk groups. The standard provides link identification, status monitoring and synchronization across links.	
Timeout	Timeout is the time interval between the individual port exchanges of LACP packets in order to check that the peer port in the trunk group is still up. If a port does not respond after three tries, then it is deemed to be "down" and is removed from the trunk. Set a short timeout (one second) for busy trunked links to ensure that disabled ports are removed from the trunk group as soon as possible. Select either 1 second or 30 seconds.	
802.1x	Select this checkbox to permit 802.1x authentication on this port. You must first allow 802.1x authentication on the switch (see *Switch Setup* screen) before configuring it on each port.	
Reauthentication	Specify if a subscriber has to periodically re-enter his or her username and password to stay connected to the port.	**On**
Reauthentication Timer	Specify how often a client has to re-enter his or her username and password to stay connected to the port.	3600
Click **Apply** to save your changes back to the switch or click **Cancel** to begin configuring this screen afresh.		

Part IV

Advanced Applications

This part shows you how to configure the Advanced Applications screens.

Chapter 7
Static Route Setup

Static routes tell the ES-3024 how to forward IP traffic when you configure the TCP/IP parameters manually.

7.1 Static Route Setup

Click **Static Route Setup** from the navigation panel to display the following static route summary table.

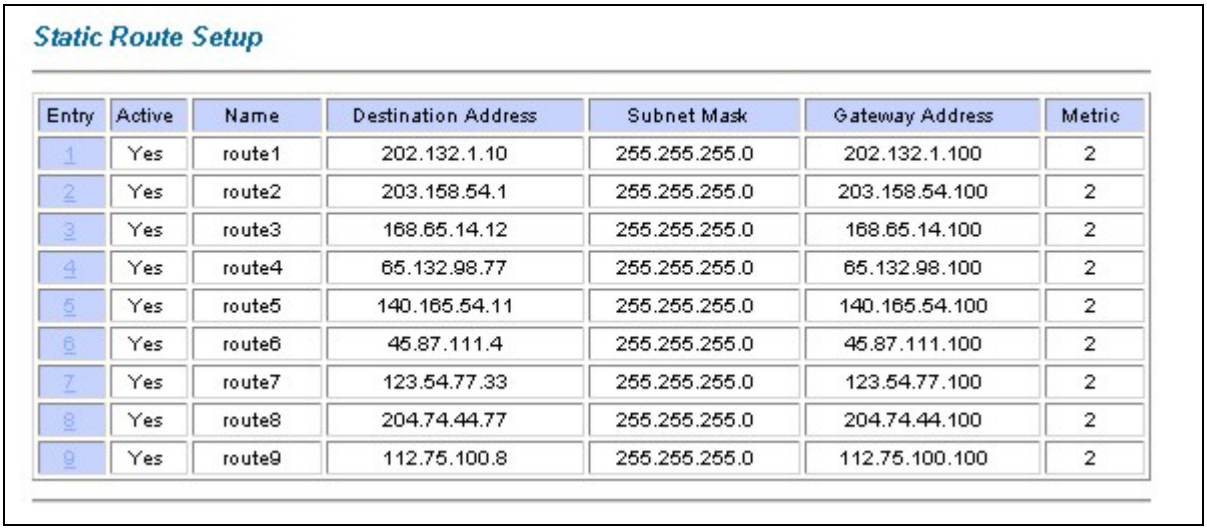

Figure 7-1 Static Route Setup

Table 7-1 Static Route Setup

LABEL	DESCRIPTION
Entry	This field displays the index number of the route.
Active	This field displays **Yes** when the static route is activated and **No** when is it deactivated.
Name	This field displays the descriptive name for this route. This is for identification purpose only.
Destination Address	This field displays the IP network address of the final destination.
Subnet Mask	This field displays the subnet mask for this destination.
Gateway Address	This field displays the IP address of the gateway. The gateway is an immediate neighbor of your switch that will forward the packet to the destination.
Metric	This field displays the cost of transmission for routing purposes.

7.2 Static Route Edit Setup

To set up a static route on the switch, click a static route index number.

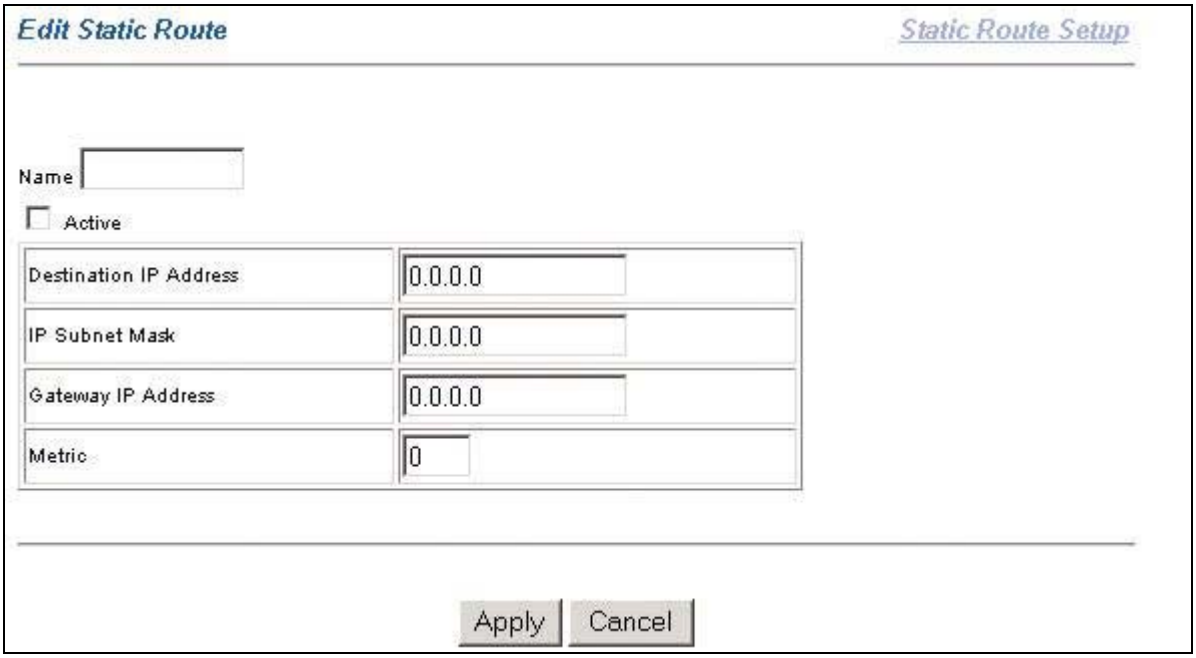

Figure 7-2 Static Route Edit Setup

Table 7-2 Static Route Edit Setup

LABEL	DESCRIPTION
Name	Enter a descriptive name for this route. This is for identification purpose only.
Active	This field allows you to activate/deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the subnet mask for this destination.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your switch that will forward the packet to the destination. The gateway must be a router on the same segment as your switch.
Metric	The metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Click **Apply** to save your changes back to the switch or click **Cancel** to begin configuring this screen afresh.	

Chapter 8
VLAN Setup

*They type of screen you see here depends on the **VLAN Type** you selected in the **Switch Setup** screen. This chapter shows you how to configure 802.1Q tagged and port-based VLANs. See the General, Switch and IP Setup chapter for more information.*

8.1 Introduction to IEEE 802.1Q Tagged VLAN

Tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges - they are not confined to the switch on which they were created. The VLANs can be created statically by hand or dynamically through GVRP. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is four bytes longer than an untagged frame and contains two bytes of TPID (Tag Protocol Identifier, residing within the type/length field of the Ethernet frame) and two bytes of TCI (Tag Control Information, starts after the source address field of the Ethernet frame).

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4,096 (212) VLANs. Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094

TPID 2 Bytes	User Priority 3 Bits	CFI 1 Bit	VLAN ID 12 bits

8.1.1 Forwarding Tagged and Untagged Frames

Each port on the switch is capable of passing tagged or untagged frames. To forward a frame from an 802.1Q VLAN-aware switch to an 802.1Q VLAN-unaware switch, the switch first decides where to forward the frame and then strips off the VLAN tag. To forward a frame from an 802.1Q VLAN-unaware switch to an 802.1Q VLAN-aware switch, the switch first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port's default VID. The default PVID is VLAN 1 for all ports, but this can be changed.

8.1.2 Automatic VLAN Registration

GARP and GVRP are the protocols used to automatically register VLAN membership across switches.

GARP

GARP (Generic Attribute Registration Protocol) allows network switchs to register and de-register attribute values with other GARP participants within a bridged LAN. GARP is a protocol that provides a generic mechanism for protocols that serve a more specific application, for example, GVRP.

GARP Timers

Switches join VLANs by making a declaration. A declaration is made by issuing a Join message using GARP. Declarations are withdrawn by issuing a Leave message. A Leave All message terminates all registrations. GARP timers set declaration timeout values.

GVRP

GVRP (GARP VLAN Registration Protocol) is a registration protocol that defines a way for switches to register necessary VLAN members on ports across the network. Enable this function to permit VLANs groups beyond the local switch.

Please refer to the following table for common GARP terminology.

Table 8-1 GARP Terminology

VLAN PARAMETER	TERM	DESCRIPTION
VLAN Type	Permanent VLAN	This is a static VLAN created manually.
	Dynamic VLAN	This is a VLAN configured by a GVRP registration/deregistration process.
VLAN Administrative Control	Registration Fixed	Fixed registration ports are permanent VLAN members.
	Registration Forbidden	Ports with registration forbidden are forbidden to join the specified VLAN.
	Normal Registration	Ports dynamically join a VLAN using GVRP.
VLAN Tag Control	Tagged	Ports belonging to the specified VLAN tag all outgoing frames transmitted.
	Untagged	Ports belonging to the specified don't tag all outgoing frames transmitted.
VLAN Port	Port VID	This is the VLAN ID assigned to untagged frames that this port received.
	Acceptable frame type	You may choose to accept both tagged and untagged incoming frames or just tagged incoming frames on a port.
	Ingress filtering	If set, the switch discards incoming frames for VLANs that do not have this port as a member

8.2 Configuring Tagged VLANs

Select **802.1Q** as the **VLAN Type** in the **Switch Setup** screen and then click **VLAN Setup** from the navigation panel to display the next screen.

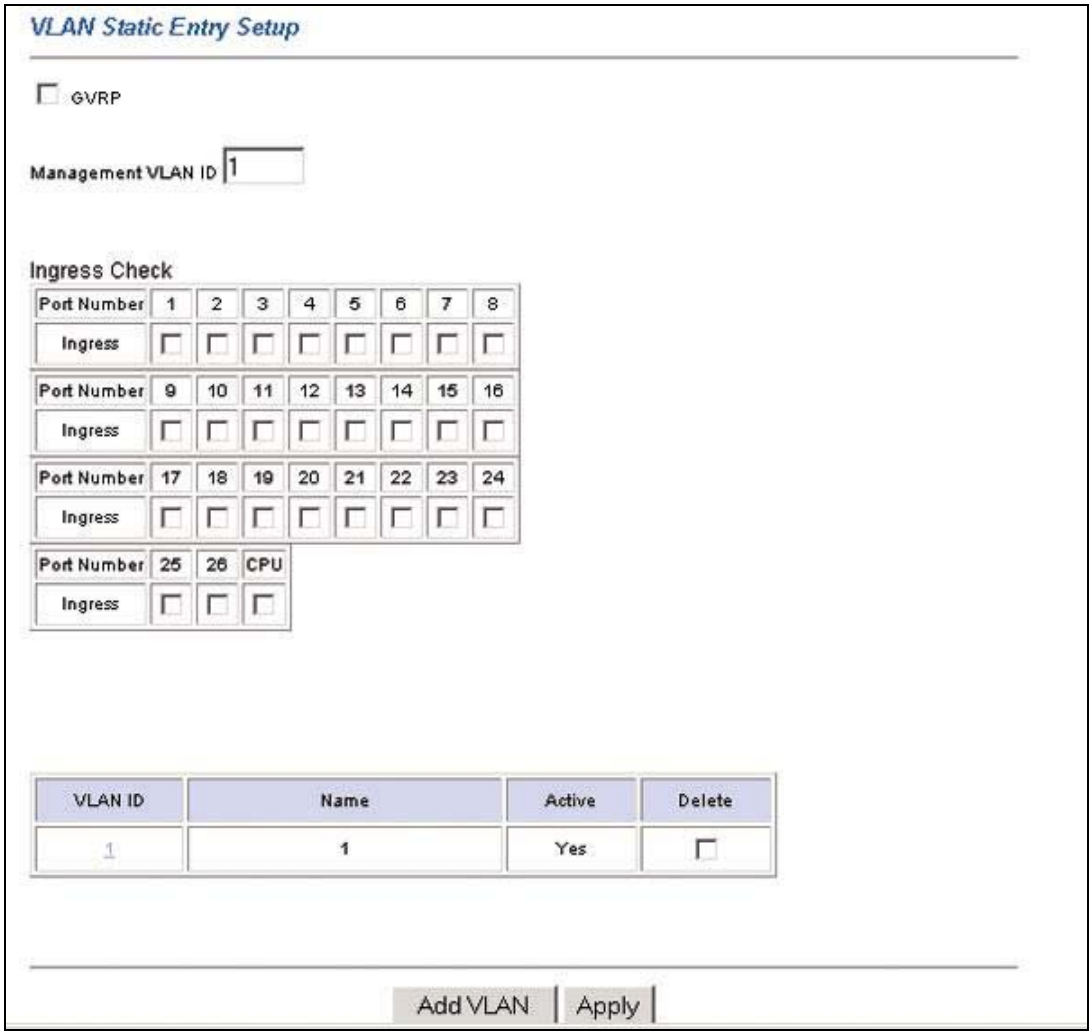

Figure 8-1 VLAN Static Entry Setup

Table 8-2 VLAN Static Entry Setup

FIELD	DESCRIPTION
GVRP	GVRP (GARP VLAN Registration Protocol) is a registration protocol that defines a way for switches to register necessary VLAN members on ports across the network. Enable this function to permit VLANs groups beyond the local switch.
Management VLAN ID	Management VLAN ID is the VLAN ID of the CPU and is used for management only. The default is "1". All ports, by default, are fixed members of this "management VLAN" in order to manage the device from any port. If a port is not a member of this VLAN, then users on that port cannot access the device. To access the device make sure the port that you are connected to is a member of Management VLAN.

Table 8-2 VLAN Static Entry Setup

FIELD	DESCRIPTION
Ingress Check	If this check box is selected for a port, the device discards incoming frames for VLANs which do not include this port in its member set.
Port Number	The **CPU** port refers to the switch management port. By default it forms a VLAN with all Ethernet ports. If it does not form a VLAN with a particular port then the switch cannot manage that port.
Ingress	Select the port(s) for which you want to perform ingress checks.
VLAN ID	The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. You may edit an existing VLAN group by clicking its ID number.
Name	This is the descriptive name for the static VLAN for identification purposes.
Active	This field displays whether this static VLAN is active or not. You can temporarily stop using a VLAN group by deactivating it rather than deleting.
Delete	To permanently stop using a VLAN group, delete it by selecting that group's **Delete** check box and then clicking **Apply**.
Click **Add VLAN** to create a new VLAN group or click **Apply** to save your changes back to the switch.	

8.2.1 Adding/Editing a VLAN Group

To edit an existing VLAN group, click its ID number under **VLAN ID** in the **VLAN Static Entry Setup** screen (*Figure 8-1*). To create a new VLAN group, click **Add VLAN** in the **VLAN Static Entry Setup** screen (*Figure 8-1*). The configuration screen for both cases is the same (*Figure 8-2*).

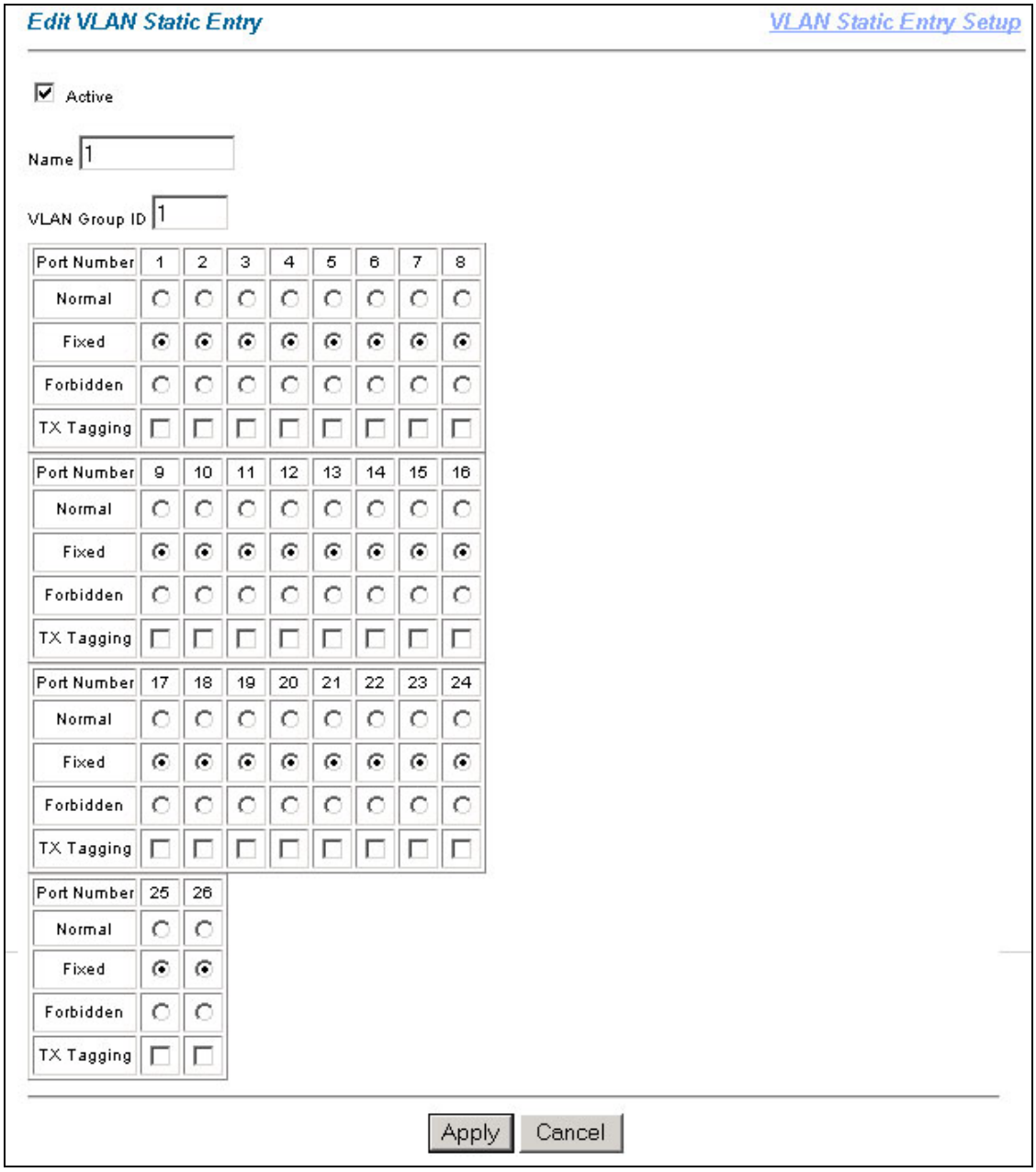

Figure 8-2 Edit VLAN Static Entry

Table 8-3 Edit VLAN Static Entry

FIELD	DESCRIPTION
Active	Select **Active** to activate this VLAN group.
Name	Enter a descriptive name (up to 12 characters) for the static VLAN for identification purposes; for example, “marketing” (without the quotes).
VLAN Group ID	Enter the VLAN ID for this static entry; the valid range is between 1 and 4094.
Port Number	The port number identifies the port you are configuring. Ports 25 and 26 are the uplink ports.
Normal	Select **Normal** for the port to dynamically join this VLAN group using GVRP.
Fixed	Select **Fixed** for the port to be a permanent member of this VLAN group.

Table 8-3 Edit VLAN Static Entry

FIELD	DESCRIPTION
Forbidden	Select **Forbidden** if you want to prohibit the port from joining this VLAN group.
TX Tagging	Select **TX Tagging** if you want the port to tag all outgoing frames transmitted with this VLAN Group ID.
Click **Apply** to save your changes back to the switch or click **Cancel** to begin configuring this screen afresh.	

8.3 Introduction to Port-based VLANs

Port-based VLANs are VLANs where the packet forwarding decision is based on the destination MAC address and its associated port.

Port-based VLANs require allowed outgoing ports to be defined for each port. Therefore, if you wish to allow two subscriber ports to talk to each other, for example, between conference rooms in a hotel, you must define the egress (an egress port is an outgoing port, that is, a port through which a data packet leaves) for both ports.

Port-based VLANs are specific only to the switch on which they were created.

The port-based VLAN setup screen is shown next. Port 0 (the CPU management port) forms a VLAN with all Ethernet ports.

8.4 Configuring Port-based VLANs

Select **Port-based** as the **VLAN Type** in the **Switch Setup** screen and then click **VLAN Setup** from the navigation panel to display the next screen.

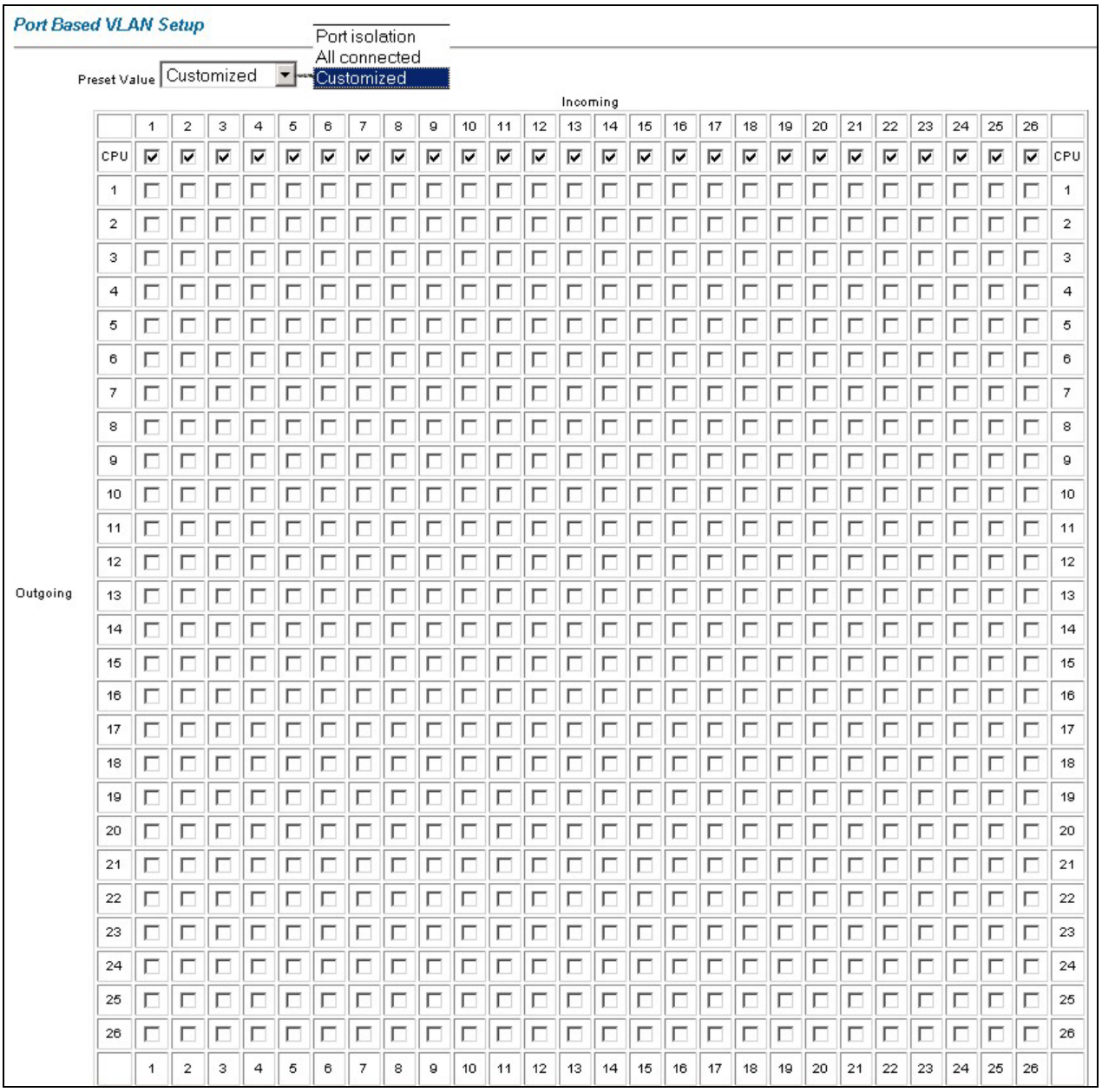
Port Based VLAN Setup
Port isolation
All connected
Customized
Preset Value
Customized
Incoming
Outgoing
CPU
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26

Figure 8-3 Port-based VLAN Setup

Table 8-4 Port-based VLAN Setup

FIELD	DESCRIPTION
Preset Value	Choose from **Port Isolation**, **All Connected** or **Customized**. **Port Isolation** means that each port (1 to 26) can only communicate with the CPU management port and cannot communicate with each other. All incoming ports are selected while only the CPU outgoing port is selected. This option is the most limiting but also the most secure. **All Connected** means all ports can communicate with each other, that is, there are no virtual LANs. All incoming and outgoing ports are selected. This option is the most flexible but also the least secure. Select **Customized** to configure specific port-based VLANs (specific only to the ES-3024). Check the ports that can communicate with each other. For two ports to communicate with each other, you must define the incoming and outgoing port for both ports. For example, for (just) ports 3 and 5 to form a VLAN, select the ports as shown in *Figure 8-4 Port-based VLAN Example*.
Incoming	These are the ingress ports; an ingress port is an incoming port, that is, a port through which a data packet enters. If you wish to allow two subscriber ports to talk to each other, you must define the ingress port for both ports. The numbers in the top row denote the incoming port for the corresponding port listed on the left (its outgoing port). **CPU** refers to the switch management port. By default it forms a VLAN with all Ethernet ports. If it does not form a VLAN with a particular port then the switch cannot be managed from that port.
Outgoing	These are the egress ports; an egress port is an outgoing port, that is, a port through which a data packet leaves. If you wish to allow two subscriber ports to talk to each other, you must define the egress port for both ports. **CPU** refers to the switch management port. By default it forms a VLAN with all Ethernet ports. If it does not form a VLAN with a particular port then the switch cannot be managed from that port.
Click **Apply** to save your changes back to the switch or click **Cancel** to begin configuring this screen afresh.	

8.4.1 Port-based VLAN Example

First select **Customized** as the **Preset Value** and then select the ports as shown for ports 3 and 5 to be in the same VLAN group.

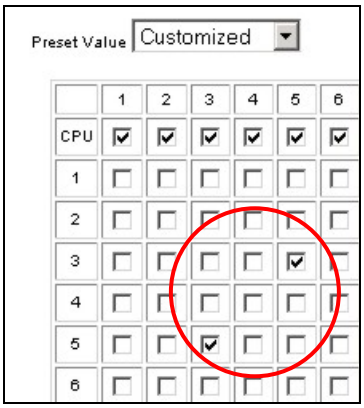

Figure 8-4 Port-based VLAN Example

Chapter 9
Static MAC Forward Setup

Use these screens to configure static MAC address forwarding.

9.1 Introduction to Static MAC Forward Setup

A static MAC address entry is an address that has been manually entered in the MAC address learning table. Static MAC addresses do not age out. **Static MAC Forward Setup** means setting static MAC addresses for a port. This may reduce the need for broadcasting.

Click **Static MAC Forward Setup** in the navigation panel to bring up the following read-only screen.

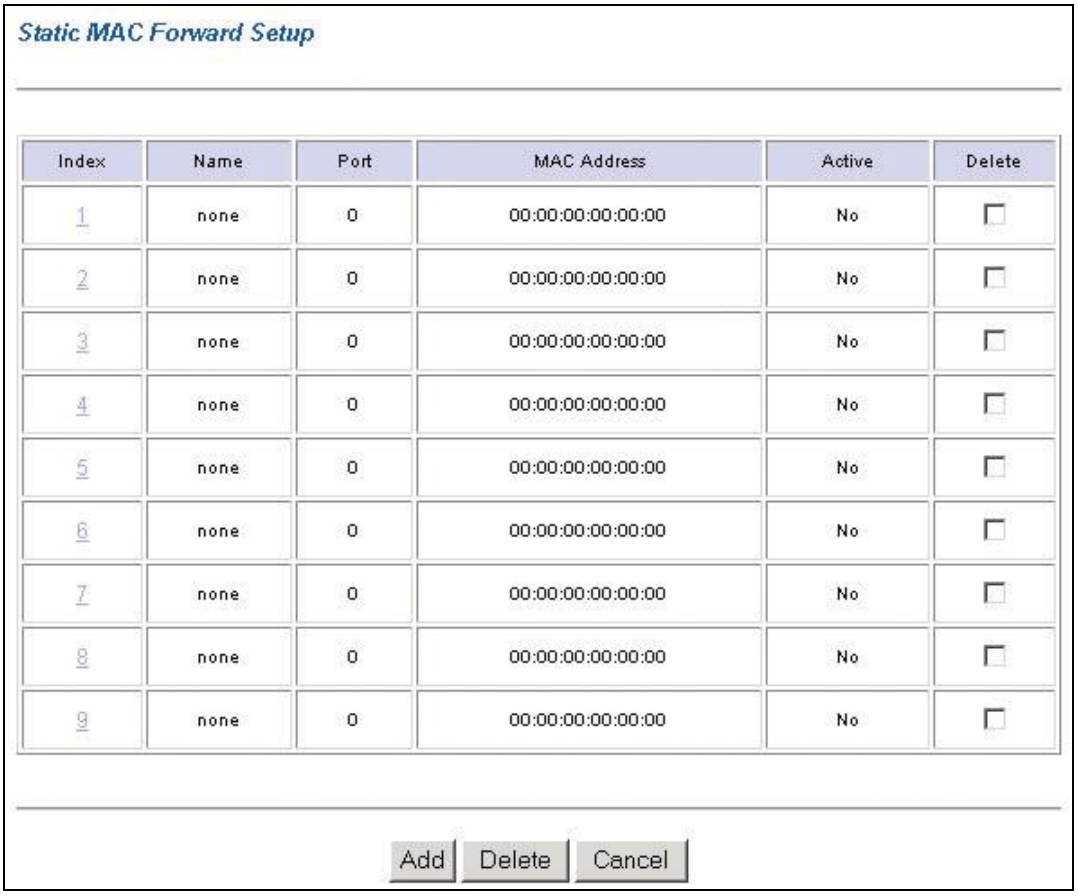

Figure 9-1 Static MAC Forward Setup

Table 9-1 Static MAC Forward Setup

FIELD	DESCRIPTION
Index	Click an index number to configure a static MAC address rule for a port.
Name	This field displays the descriptive name for identification purposes for this static MAC address-forwarding rule.

Table 9-1 Static MAC Forward Setup

FIELD	DESCRIPTION
Port	This field displays the port where the MAC address shown in the next field will be forwarded.
MAC Address	This field displays the MAC address that will be forwarded.
Active	This field displays whether this static MAC address forwarding rule is active or not. You may temporarily deactivate a rule without deleting it.
Add	To add a new static MAC address-forwarding rule, click this button.
Delete	To delete a rule, select its checkbox in the **Delete** column and then click this **Delete** button.
Cancel	Click **Cancel** to begin configuring this screen afresh.

9.2 Configuring or Editing a Static MAC Forward Rule

Click **Add** to configure a new rule or click an index number to edit an existing static MAC address rule. Either way, a screen as shown next is displayed.

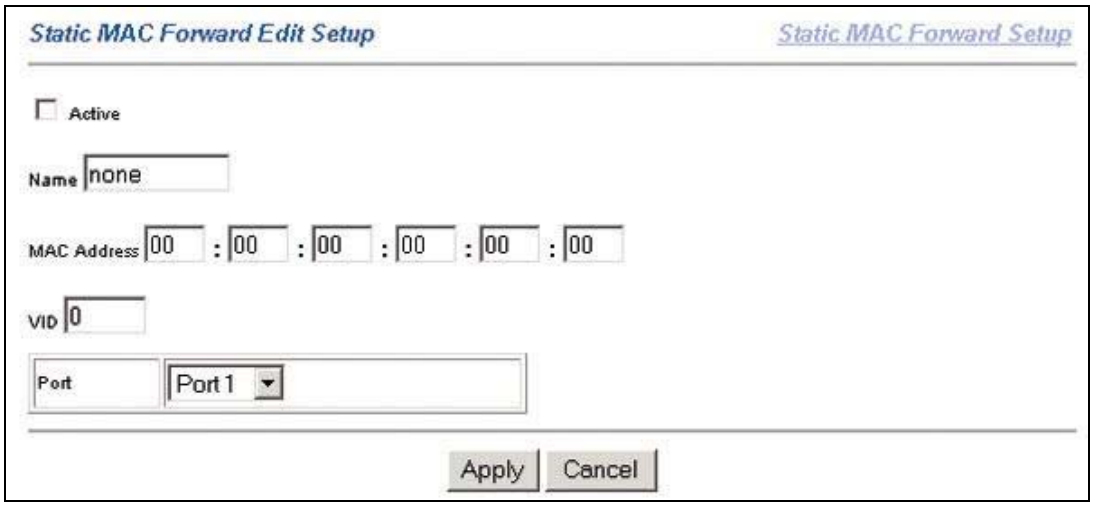

Figure 9-2 Configuring or Editing a Static MAC Forward Rule

Table 9-2 Configuring or Editing a Static MAC Forward Rule

FIELD	DESCRIPTION
Active	Make sure to select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by deselecting this check box.
Name	Type descriptive name for identification purposes for this static MAC address forwarding rule.
MAC Address	Type the MAC address in valid MAC address format, that is, six hexadecimal character pairs. Static MAC addresses do not age out.
VID	Type the VLAN identification number.
Port	Select a port where the MAC address entered in the previous field will be automatically forwarded.
Click **Apply** to save your changes back to the switch or click **Cancel** to begin configuring this screen afresh.	

Chapter 10
Filter Setup

This chapter discusses static MAC address port filtering.

10.1 Introduction to Port Filtering

Port filtering means sifting traffic from one or all ports to one or all ports based on the source and/or destination MAC addresses and VLAN group.

Click **Filter Setup** from the navigation panel to bring up the next port filter summary screen.

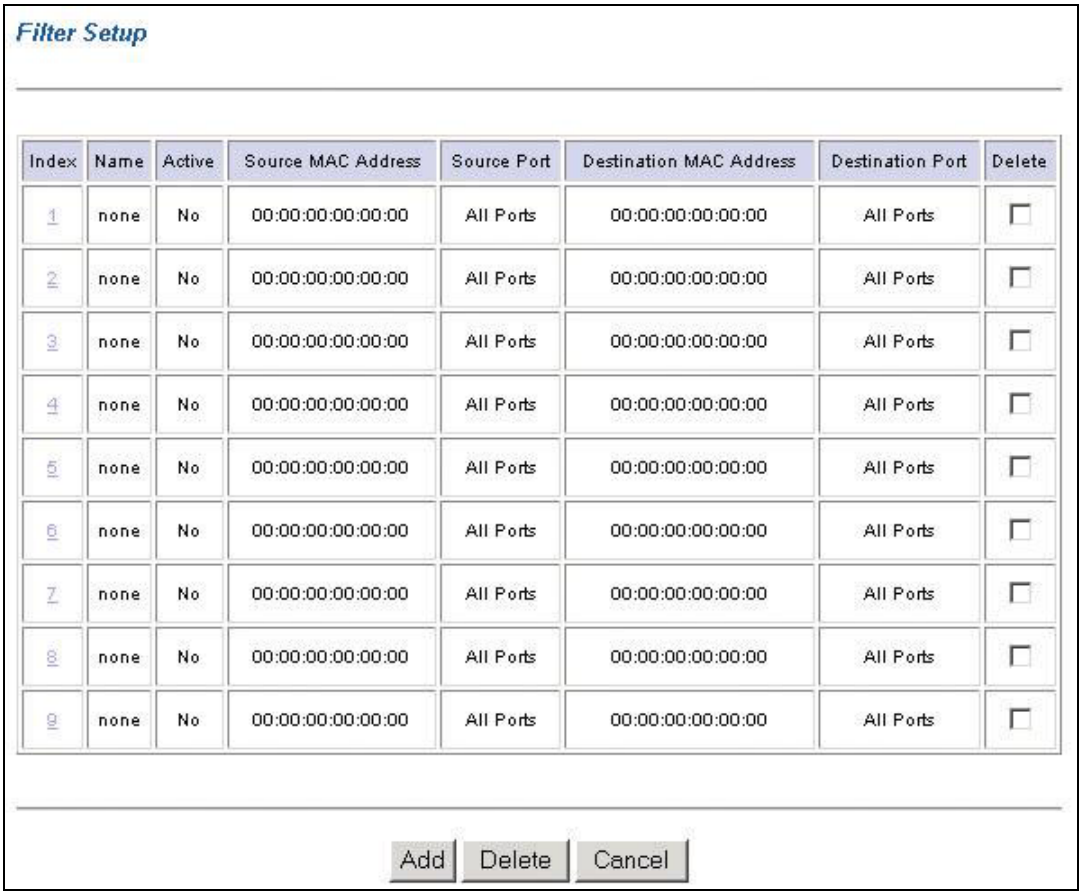
Filter Setup
Index
Name
Active
Source MAC Address
Source Port
Destination MAC Address
Destination Port
Delete
1 none No 00:00:00:00:00:00 All Ports 00:00:00:00:00:00 All Ports
2 none No 00:00:00:00:00:00 All Ports 00:00:00:00:00:00 All Ports
3 none No 00:00:00:00:00:00 All Ports 00:00:00:00:00:00 All Ports
4 none No 00:00:00:00:00:00 All Ports 00:00:00:00:00:00 All Ports
5 none No 00:00:00:00:00:00 All Ports 00:00:00:00:00:00 All Ports
6 none No 00:00:00:00:00:00 All Ports 00:00:00:00:00:00 All Ports
7 none No 00:00:00:00:00:00 All Ports 00:00:00:00:00:00 All Ports
8 none No 00:00:00:00:00:00 All Ports 00:00:00:00:00:00 All Ports
9 none No 00:00:00:00:00:00 All Ports 00:00:00:00:00:00 All Ports
Add
Delete
Cancel

Figure 10-1 Filter Setup

Table 10-1 Filter Setup

LABEL	DESCRIPTION
Index	This field displays the index number of the filter rule.
Name	This field displays the descriptive name for this filter rule. This is for identification purpose only.

Table 10-1 Filter Setup

LABEL	DESCRIPTION
Active	This field displays **Yes** when the filter rule is activated and **No** when is it deactivated.
Source MAC Address	This field displays the source MAC address in hexadecimal format. **All Entries** means all MAC addresses.
Source Port	This field displays the Ethernet port number from which packets are transmitted. You may choose one port only or all ports.
Destination MAC Address	This field displays the destination MAC address in hexadecimal format. **All Entries** means all MAC addresses.
Destination Port	This field displays the Ethernet port number to which packets are sent. You may choose one port only or all ports.
Delete	To delete a rule, select its checkbox in this column and then click the **Delete** button.
Add	To add a filter rule, click this button.
Delete	To delete a rule, select its checkbox in the **Delete** column and then click this **Delete** button.
Cancel	Click **Cancel** to begin configuring this screen afresh.

10.2 Configuring or Editing a Filter Rule

Click **Add** to configure a new filter rule or click an index number to edit an existing filter rule. Either way, a screen as shown next is displayed.

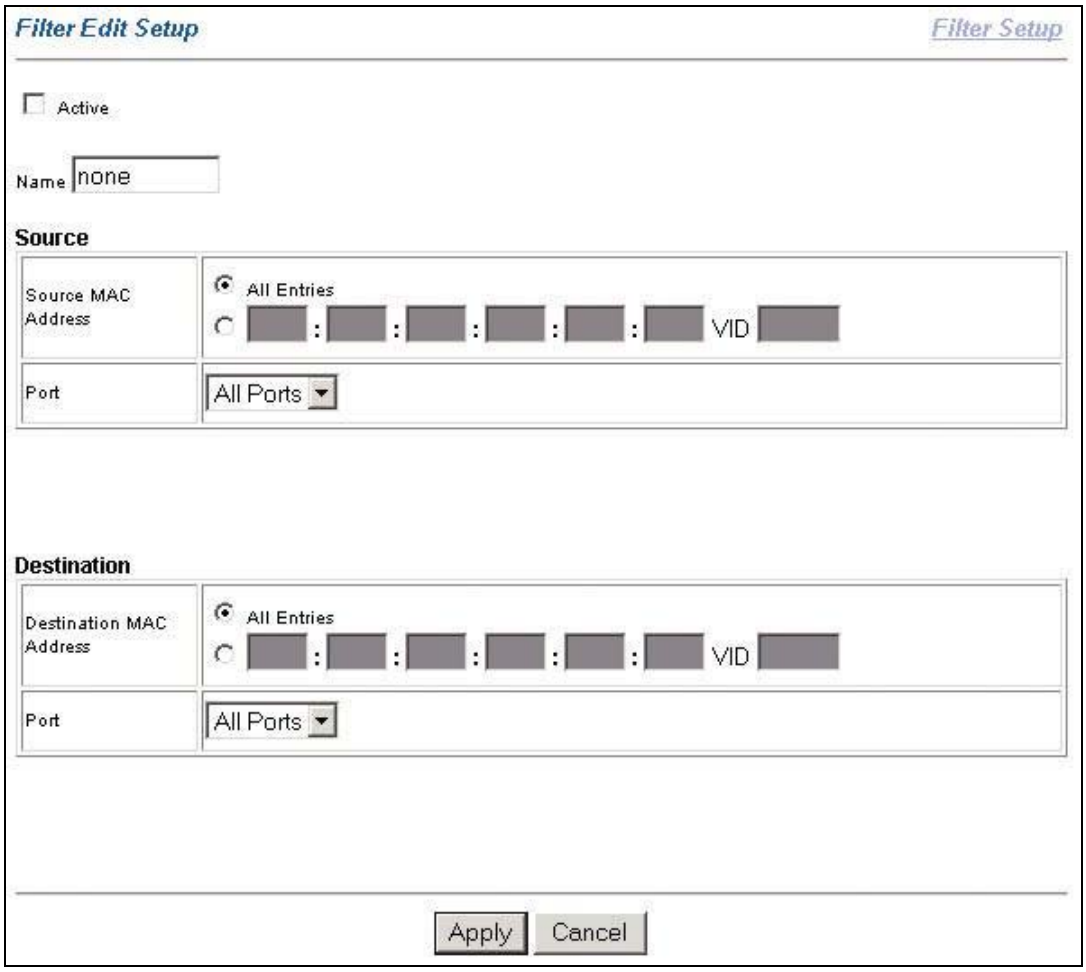

Figure 10-2 Configuring or Editing a Filter Rule

Table 10-2 Configuring or Editing a Filter Rule

LABEL	DESCRIPTION
Active	Make sure to select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by deselecting this check box.
Name	Type a descriptive name for this filter rule. This is for identification purpose only.
Source	The next three fields pertain to the source MAC address and source port.
Source MAC Address	Type a MAC address in valid MAC address format, that is, six hexadecimal character pairs or click **All Entries** to apply the filter rule to all MAC addresses.
VID	Type the VLAN group identification number.
Port	Select the port to which the filter rule should be applied. You may choose one port only or all ports (**All Ports**).
Destination	The next three fields pertain to the destination MAC address and destination port.

Table 10-2 Configuring or Editing a Filter Rule

LABEL	DESCRIPTION
MAC Address	Type a MAC address in valid MAC address format, that is, six hexadecimal character pairs or click **All Entries** to apply the filter rule to all MAC addresses.
VID	Type the VLAN group identification number.
Port	Select the port to which the filter rule should be applied. You may choose one port only or all ports (**All Ports**).
Click **Apply** to save your changes back to the switch or click **Cancel** to begin configuring this screen afresh.	

Chapter 11 Mirror Setup

This chapter discusses the Mirror setup screens.

11.1 Introduction to Port Mirroring

Port mirroring allows you to copy traffic going from one or all ports to another or all ports in order that you can examine the traffic from the mirror port (the port you copy the traffic to) without interference.

Click **Mirror Setup** in the navigation panel to bring up the next mirror setup summary screen.

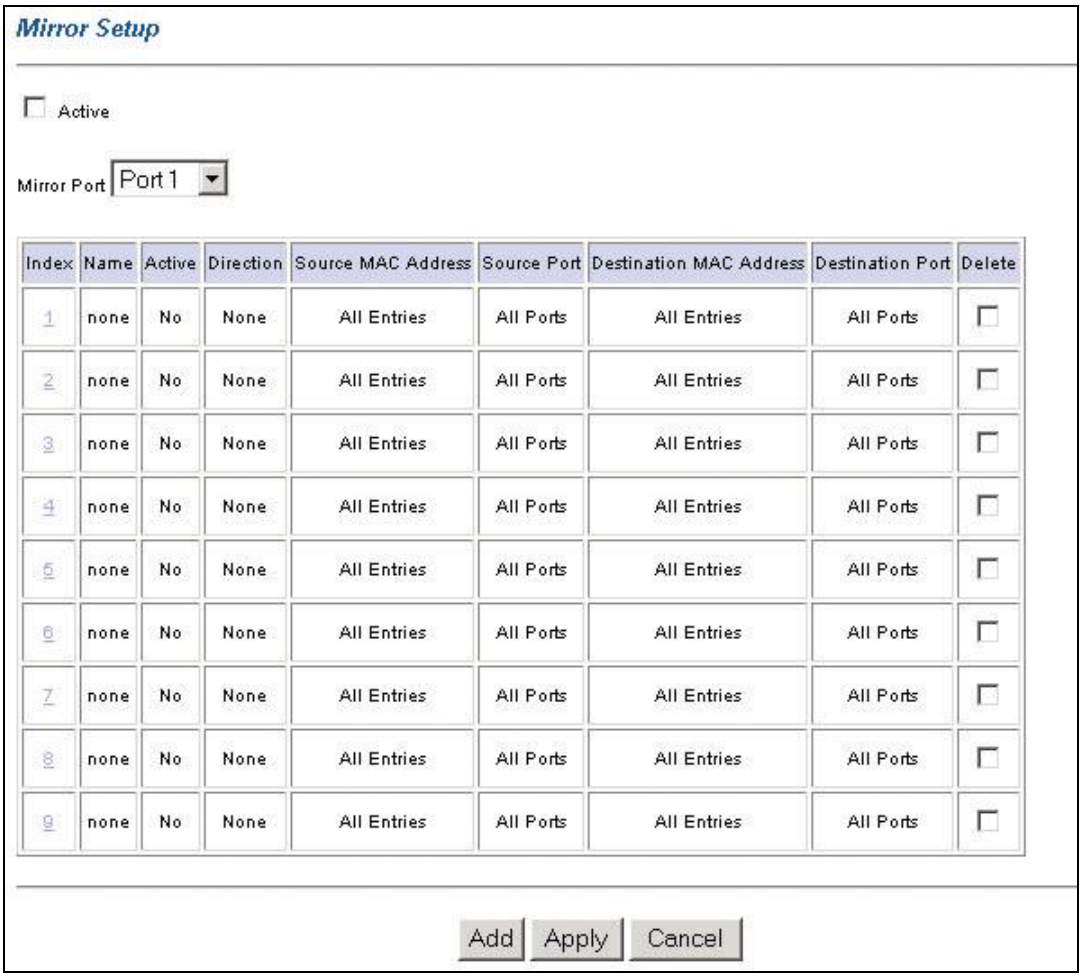
Mirror Setup
Active
Mirror Port
Port 1
Index
Name
Active
Direction
Source MAC Address
Source Port
Destination MAC Address
Destination Port
Delete
1 none No None All Entries All Ports All Entries All Ports
2 none No None All Entries All Ports All Entries All Ports
3 none No None All Entries All Ports All Entries All Ports
4 none No None All Entries All Ports All Entries All Ports
5 none No None All Entries All Ports All Entries All Ports
6 none No None All Entries All Ports All Entries All Ports
7 none No None All Entries All Ports All Entries All Ports
8 none No None All Entries All Ports All Entries All Ports
9 none No None All Entries All Ports All Entries All Ports
Add
Apply
Cancel

Figure 11-1 Mirror Setup

Table 11-1 Mirror Setup

LABEL	DESCRIPTION
Active	Clear this check box to deactivate port mirroring on the switch.

Table 11-1 Mirror Setup

LABEL	DESCRIPTION
Mirror Port	The mirror port is the port you copy the traffic to in order to examine it in more detail without interfering with the traffic flow on the original port(s). Select this port from this drop-down list box.
Index	This field displays the index number of the mirror rule. Click the index number to edit this mirror rule.
Name	This field displays the descriptive name for this mirror rule. This is for identification purpose only.
Active	This field displays **Yes** when the mirror rule is activated and **No** when is it deactivated.
Direction	This is the direction to which the rule applies, that is **Incoming**, **Outgoing** or **Both**.
Source MAC Address	This field displays the source MAC address in hexadecimal format. **All Entries** means all MAC addresses.
Source Port	This field displays the Ethernet port number from which packets are transmitted. You may choose one port only or all ports.
Destination MAC Address	This field displays the destination MAC address in hexadecimal format. **All Entries** means all MAC addresses.
Destination Port	This field displays the Ethernet port number to which packets are sent. You may choose one port only or all ports.
Delete	To delete a rule, select its checkbox in this column and then click the **Apply** button.
Add	To add a mirror rule, click this button.
Click **Apply** to save your changes back to the switch or click **Cancel** to begin configuring this screen afresh.	

11.2 Configuring or Editing a Mirror Rule

Click **Add** to configure a new mirror rule or click an index number to edit an existing mirror rule. Either way, a screen as shown next is displayed.

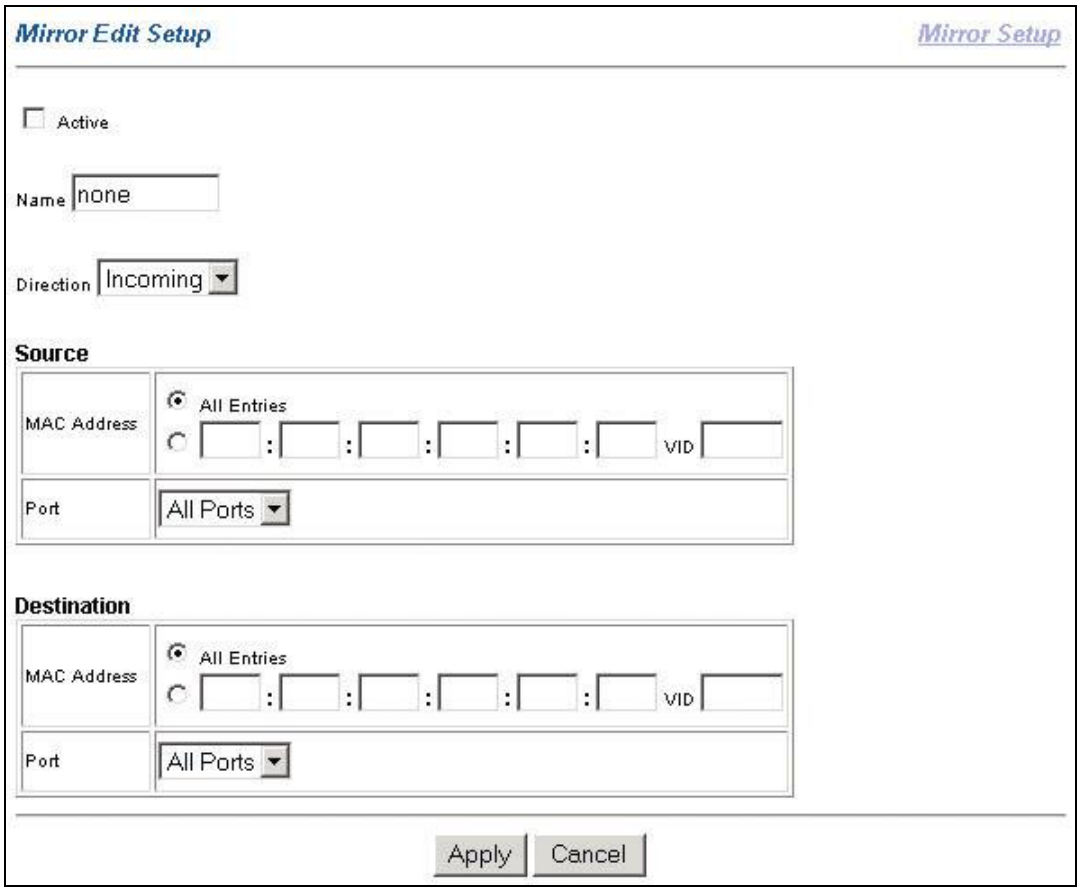

Figure 11-2 Configuring or Editing a Mirror Rule

Table 11-2 Configuring or Editing a Mirror Rule

LABEL	DESCRIPTION
Active	Make sure to select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by clearing this check box.
Name	Type a descriptive name for this mirror rule. This is for identification purposes only.
Direction	Choose the direction to which the rule applies from **Incoming**, **Outgoing** or **Both**.
Source	The source and destination fields identify the traffic you want to copy for analysis. You can identify source-destination traffic through a combination of MAC address, VLAN group and port. Configure these parameters in the next three fields.
MAC Address	Type a MAC address in valid MAC address format, that is, six hexadecimal character pairs or click **All Entries** to apply the filter rule to all MAC addresses.
VID	Type the VLAN group identification number.
Port	Select the port to which the filter rule should be applied. You may choose one port only or all ports (**All Ports**).

Table 11-2 Configuring or Editing a Mirror Rule

LABEL	DESCRIPTION
Destination	The source and destination fields identify the traffic you want to copy for analysis. You can identify source-destination traffic through a combination of MAC address, VLAN group and port. Configure these parameters in the next three fields.
MAC Address	Type a MAC address in valid MAC address format, that is, six hexadecimal character pairs or click **All Entries** to apply the filter rule to all MAC addresses.
VID	Type the VLAN group identification number.
Port	Select the port to which the filter rule should be applied. You may choose one port only or all ports (**All Ports**).
Click **Apply** to save your changes back to the switch or click **Cancel** to begin configuring this screen afresh.	

Chapter 12
Bandwidth Control Setup

This chapter shows you how you can cap the maximum bandwidth allowed from specific source(s) to specified destination(s) using the Bandwidth Control setup screens.

12.1 Introduction to Bandwidth Control

Bandwidth control means defining a maximum allowable bandwidth for traffic flows from specified source(s) to specified destination(s). Click **Bandwidth Control Setup** from the navigation panel to bring up the next screen.

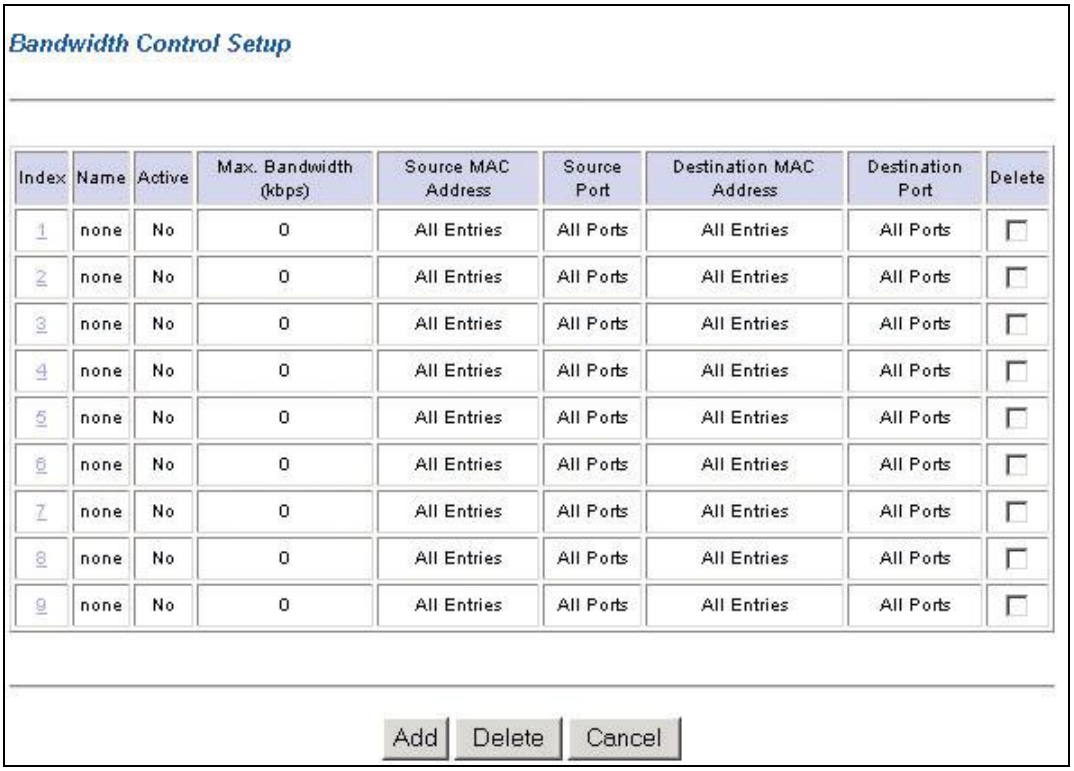
Bandwidth Control Setup
Index
Name
Active
Max. Bandwidth (kbps)
Source MAC Address
Source Port
Destination MAC Address
Destination Port
Delete
1 none No 0 All Entries All Ports All Entries All Ports
2 none No 0 All Entries All Ports All Entries All Ports
3 none No 0 All Entries All Ports All Entries All Ports
4 none No 0 All Entries All Ports All Entries All Ports
5 none No 0 All Entries All Ports All Entries All Ports
6 none No 0 All Entries All Ports All Entries All Ports
7 none No 0 All Entries All Ports All Entries All Ports
8 none No 0 All Entries All Ports All Entries All Ports
9 none No 0 All Entries All Ports All Entries All Ports
Add
Delete
Cancel

Figure 12-1 Bandwidth Control Setup

Table 12-1 Bandwidth Control Setup

LABEL	DESCRIPTION
Index	This field displays the index number of the rule. Click an index number to edit that rule.
Name	This field displays the descriptive name for this rule. This is for identification purposes only.
Active	This field displays whether the bandwidth control rule is activated or not.

Table 12-1 Bandwidth Control Setup

LABEL	DESCRIPTION
Max. Bandwidth (kbps)	This field displays the maximum bandwidth allowed in kilobits per second for this traffic flow.
Source MAC Address	This field displays the source MAC address in hexadecimal format. **All Entries** means all MAC addresses.
Source Port	This field displays the Ethernet port number from which packets are transmitted. You may choose one port only or all ports.
Destination MAC Address	This field displays the destination. MAC address in hexadecimal format. **All Entries** means all MAC addresses.
Destination Port	This field displays the Ethernet port number to which packets are sent. You may choose one port only or all ports.
Delete	To delete a rule, select its checkbox in this column and then click the **Delete** button.
Add	To add a rule, click this button.
Delete	To delete a rule, select its checkbox in the **Delete** column and then click this **Delete** button.
Cancel	Click **Cancel** to begin configuring this screen afresh.

12.2 Configuring or Editing a Bandwidth Control Rule

Click **Add** to configure a new rule or click an index number to edit an existing Bandwidth Control setup rule. Either way, a screen as shown next is displayed.

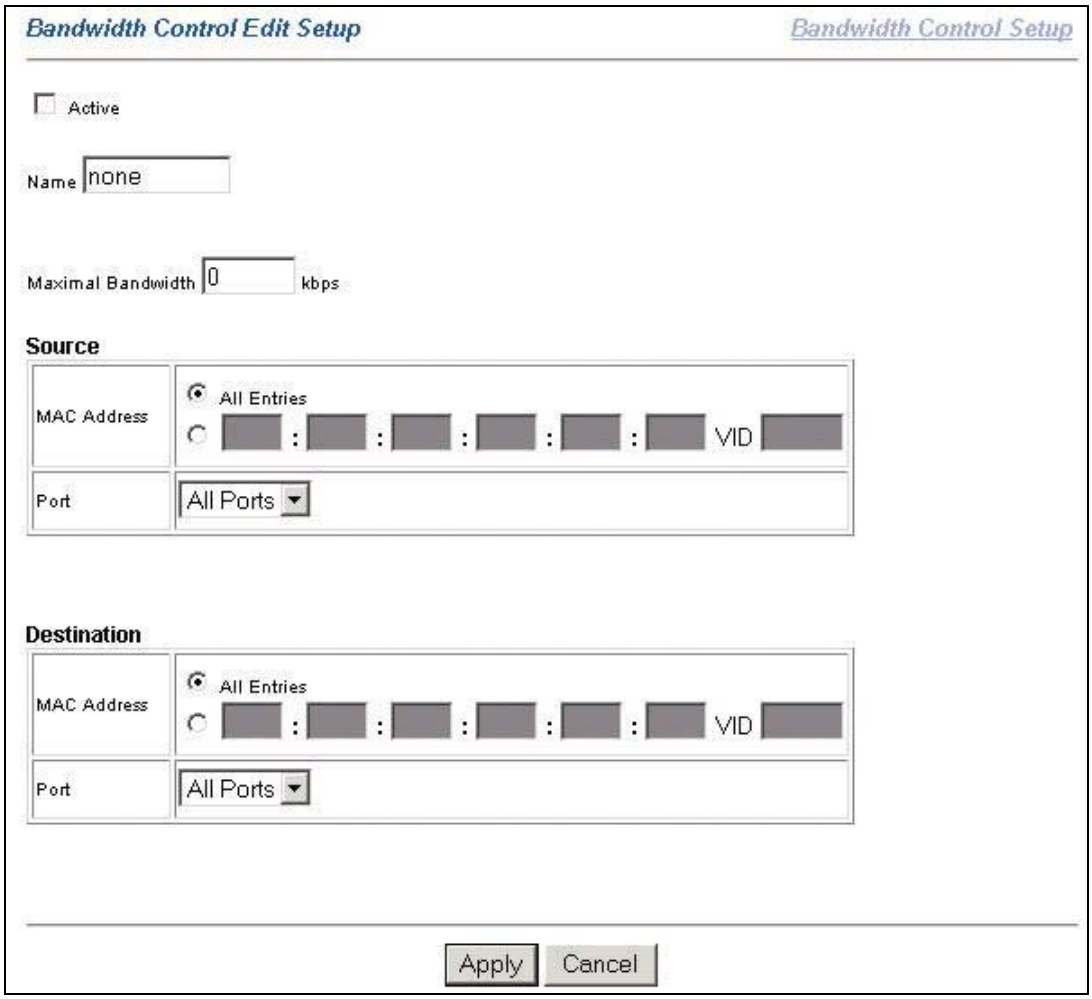

Figure 12-2 Bandwidth Control Setup Edit

Table 12-2 Bandwidth Control Setup Edit

LABEL	DESCRIPTION
Active	Make sure to select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by clearing this check box.
Name	Type a descriptive name for this bandwidth control rule. This is for identification purpose only.
Maximum Bandwidth	Type the maximum bandwidth allowed in kilobits per second for this traffic flow.
Source	The next three fields pertain to the source MAC address and source port.
MAC Address	Type a MAC address in valid MAC address format, that is, six hexadecimal character pairs or click **All Entries** to apply the filter rule to all MAC addresses.
VID	Type the VLAN group identification number.
Port	Select the port to which the bandwidth control rule should apply. You may choose one port only or all ports (**All Ports**).

Table 12-2 Bandwidth Control Setup Edit

LABEL	DESCRIPTION
Destination	The next three fields pertain to the destination MAC address and destination port.
MAC Address	Type a MAC address in valid MAC address format, that is, six hexadecimal character pairs or click **All Entries** to apply the filter rule to all MAC addresses.
VID	Type the VLAN identification number.
Port	Select the port to which the bandwidth control rule should apply. You may choose one port only or all ports (**All Ports**).
Click **Apply** to save your changes back to the switch or click **Cancel** to begin configuring this screen afresh.	

Chapter 13 Trunk Setup

This chapter shows you how to logically aggregate physical links to form one logical, higher-bandwidth link.

13.1 Introduction to Trunking

Trunking (link aggregation) is the grouping of physical ports into one logical higher-capacity link. You may want to trunk ports if for example, it is cheaper to use multiple lower-speed links than to under-utilize a high-speed, but more costly, single-port link.

However, the more ports you aggregate then the fewer available ports you have. You may configure up to four trunk groups in the ES-3024. A trunk group is one logical link containing multiple ports.

Ports should be physically linked in consecutive order without gaps when forming trunk groups. For example ports 9, 10, 11 and 12 in switch 1 should connect to ports 1, 2, 3 and 4 in switch 2 to form one trunk group; ports 9, 10, 11 and 12 in switch 1 connected to ports 1, 3, 2, 4 in switch 2 would form two trunk groups, not one.

Table 13-1 Trunk Groups

TRUNK GROUP	BEGINNING-TO-END PORT RANGE
T1	1 to 8
T2	9 to 16
T3	17 to 24
T4	25 and 26 (the uplink ports)

See also the **Switch Setup** chapter for information on dynamic link aggregation using the Link Aggregation Control Protocol (LACP). The ES-3024 adheres to the 802.3ad standard for static and dynamic (LACP) port trunking.

13.2 Trunk Setup

Click **Trunk Setup** in the navigation panel to display the screen shown next.

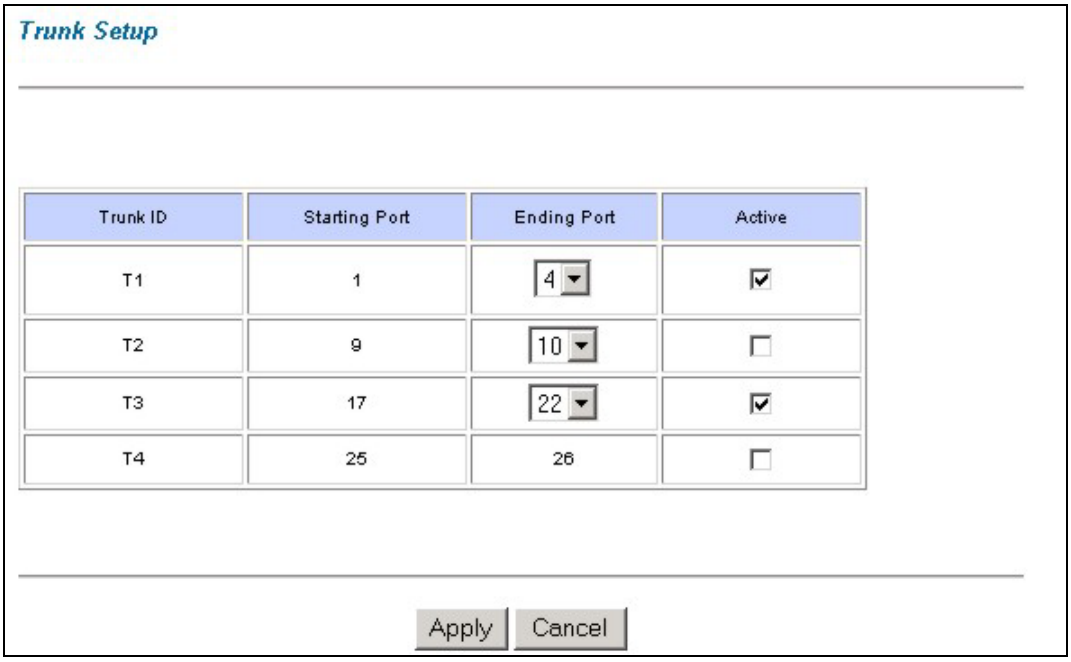

Figure 13-1 Trunk Setup

Table 13-2 Trunk Setup

LABEL	DESCRIPTION
Trunk ID	The trunk ID identifies the trunk group, that is, one logical link containing multiple ports – see *Table 13-1 Trunk Groups*.
Starting Port	This is the beginning port in the trunk group's port range and is not configurable - see *Table 13-1 Trunk Groups*.
Ending Port	Select the end port in the port range from the drop-down list box - see *Table 13-1 Trunk Groups*.
Active	Make sure to select this check box to activate the trunk group. You may temporarily deactivate a trunk group without deleting it by clearing this check box.
Click **Apply** to save your changes back to the switch or click **Cancel** to begin configuring this screen afresh.	

Part V

Advanced Management

This part describes the advanced management screens.

Chapter 14 SNMP

This chapter discusses SNMP (Simple Network Management Protocol) for network management and monitoring.

14.1 About SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network switches. SNMP is a member of TCP/IP protocol suite. A manager station can manage and monitor the ES-3024 through the network via SNMP version one (SNMPv1) and/or SNMP version 2c. The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

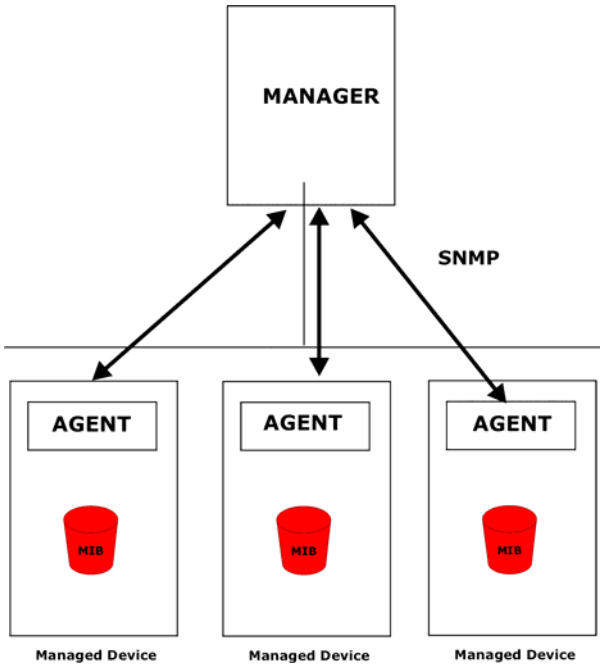

Figure 14-1 SNMP Management Model

An SNMP managed network consists of two main components: agents and a manager.

An agent is a management software module that resides in a managed switch (the ES-3024). An agent translates the local management information from the managed switch into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a switch. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

Table 14-1 SNMP Commands

COMMAND	DESCRIPTION
Get	Allows the manager to retrieve an object variable from the agent.
GetNext	Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
Set	Allows the manager to set values for object variables within an agent.
Trap	Used by the agent to inform the manager of some events.

14.2 Supported MIBs

MIBs let administrators collect statistics and monitor status and performance.

The ES-3024 supports the following MIBs:

- SNMP MIB II (RFC 1213)
- RFC 1493 Bridge MIBs
- RFC 1155 SMI
- RFC 1757 RMON
- RFC 1157 SNMP v1
- RFC 1643 Ethernet MIBs
- RFC 2674 SNMPv2, SNMPv2c
- SNMPv2, SNMPv2c or later version, compliant with RFC 2011 SNMPv2 MIB for IP, RFC 2012 SNMPv2 MIB for TCP, RFC 2013 SNMPv2 MIB for UDP

14.3 Configuring SNMP

To configure SNMP, click **SNMP** from the navigation panel. The "community" for **Get**, **Set** and **Trap** fields is simply SNMP's terminology for password.

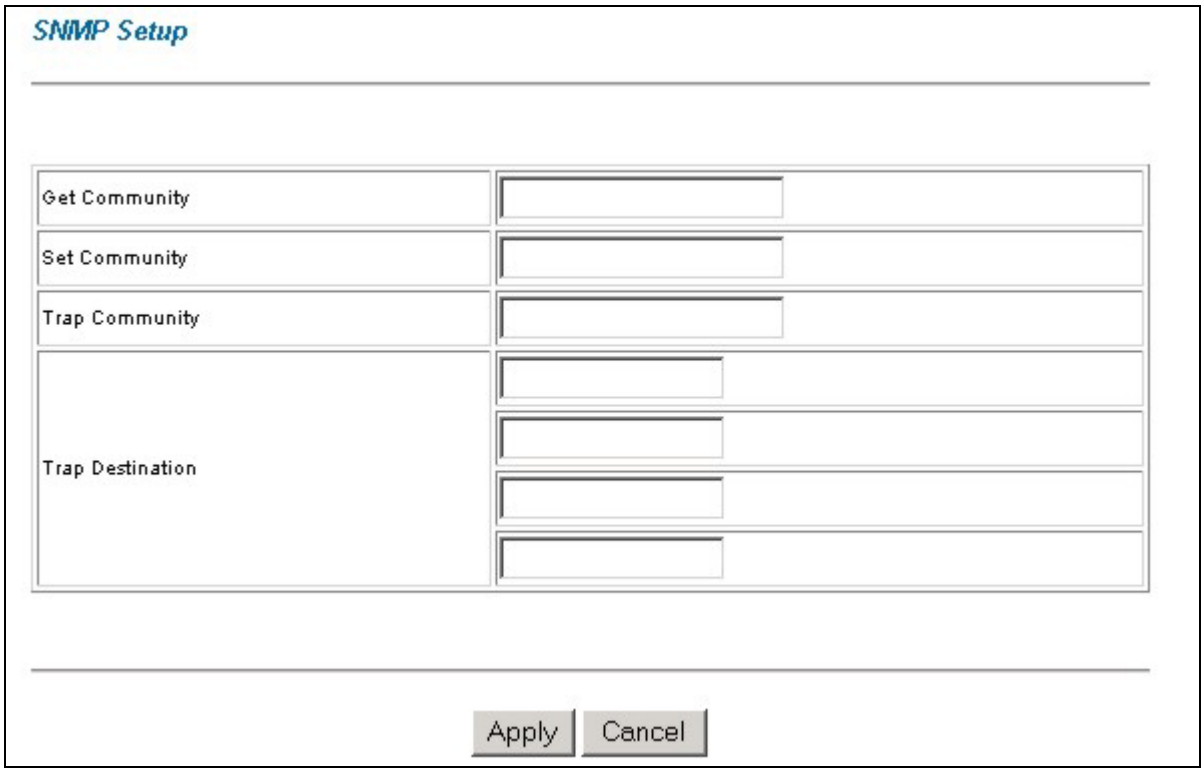

Figure 14-2 SNMP Setup

The following table describes the SNMP configuration parameters.

Table 14-2 SNMP Setup

LABEL	DESCRIPTION
Get Community	Enter the get community, which is the password for the incoming Get- and GetNext- requests from the management station.
Set Community	Enter the set community, which is the password for incoming Set- requests from the management station.
Trap: Community	Enter the trap community, which is the password sent with each trap to the SNMP manager.
Trap: Destination	Enter the IP addresses of up to four stations to send your SNMP traps to.
Click **Apply** to save your changes back to the switch or click **Cancel** to begin configuring this screen afresh.	

14.4 SNMP Traps

The ES-3024 sends traps to an SNMP manager when an event occurs. SNMP traps supported are outlined in the following table.

Table 14-3 SNMP Traps

GENERIC TRAP	SPECIFIC TRAP	DESCRIPTION
0 (Cold Start)	0	This trap is sent when the ES-3024 is turned on.
1 (WarmStart)	0	This trap is sent when the ES-3024 restarts.

Table 14-3 SNMP Traps

GENERIC TRAP	SPECIFIC TRAP	DESCRIPTION
2 (linkDown)	0	This trap is sent when the Ethernet is down.
3 (linkUp)	0	This trap is sent when the Ethernet is up.
4 (authenticationFailure)	0	This trap is sent when an SNMP request comes from non-authenticated hosts.
6 (enterpriseSpecific)	1(TRAP_REBOOT)	This trap is sent when the system is going to reboot. The trap displays the reason for the reboot.
	2 (TRAP_SYSTEMSHUTDOWN)	This trap is sent when the system is going to shut down. The trap displays the reason for the shutdown.
	3 (TRAP_OVERHEAT)	This trap is sent when the temperature exceeds the threshold of 65 degrees centigrade. For example, the following trap shows that the current reading at Temp1 is 68 degrees centigrade. "Temp1 exceeds Limit (Limit = 65 degree C, Read = 68 degree C)"
	4 (TRAP_OVERHEATOVER)	This trap is sent when the temperature returns to normal. For example, the following trap shows that the current reading at Temp1 is 64 degrees centigrade. "Temp1 back to Normal (Limit = 65 degree C, Read = 64 degree C)"
	5 (TRAP_ERRLOG)	This trap is sent when an error log is recorded in the system. The trap includes the content of the error log.
	6 (TRAP_FANRPMLOW)	This trap is sent when the fan speed falls below 4000 RPM (“Limit”, the minimum speed allowed). For example, the following trap shows that the current reading at FAN 1 is 3800 RPM. "FAN1 exceeds Limit (Limit = 4000 RPM, Read = 3800 RPM)"
	7 (TRAP_FANRPMNORMAL)	This trap is sent when the fan speed returns to normal. For example, the following trap shows that the current reading at FAN 1 is 5500 RPM. "FAN1 back to Normal (Limit = 4000 RPM, Read = 5500 RPM)"
	8 (TRAP_VOLTAGELOW)	This trap is sent when the voltage falls out of the tolerance range. For example, the following trap shows that the current reading at the 3.3V sensor is 3.00V, the upper voltage limit is 3.36V and the lower voltage limit is 3.10V. "Power 3.3V exceeds Limit (Up Limit = 3.36V, Down Limit = 3.10V, Read = 3.00V)"

Table 14-3 SNMP Traps

GENERIC TRAP	SPECIFIC TRAP	DESCRIPTION
	9 (TRAP_POWENORMAL)	This trap is sent when the voltage returns to normal. For example, the following trap shows that the current reading at the 3.3V sensor is 3.20V, the upper voltage limit is 3.36V and the lower voltage limit is 3.10V. "Power 3.3V back to Normal (Up Limit = 3.36V, Down Limit = 3.10V, Read = 3.20V)"

Chapter 15
RADIUS Setup

This chapter shows you how to configure the RADIUS Setup screen in order to connect to an external RADIUS server.

15.1 Introduction to RADIUS

RADIUS (Remote Authentication Dial-In User Service) authentication is a popular protocol used to authenticate users by means of an external server instead of (or in addition to) an internal device user database that is limited to the memory capacity of the device. In essence, RADIUS authentication allows you to validate an unlimited number of users from a central location.

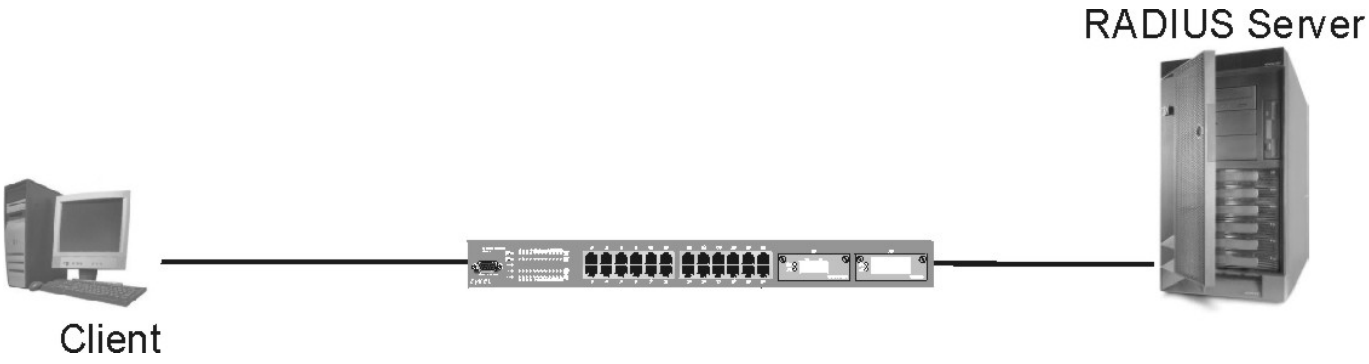

Figure 15-1 RADIUS Server

15.2 RADIUS Setup

Click **Radius** from the navigation panel to display the next screen.

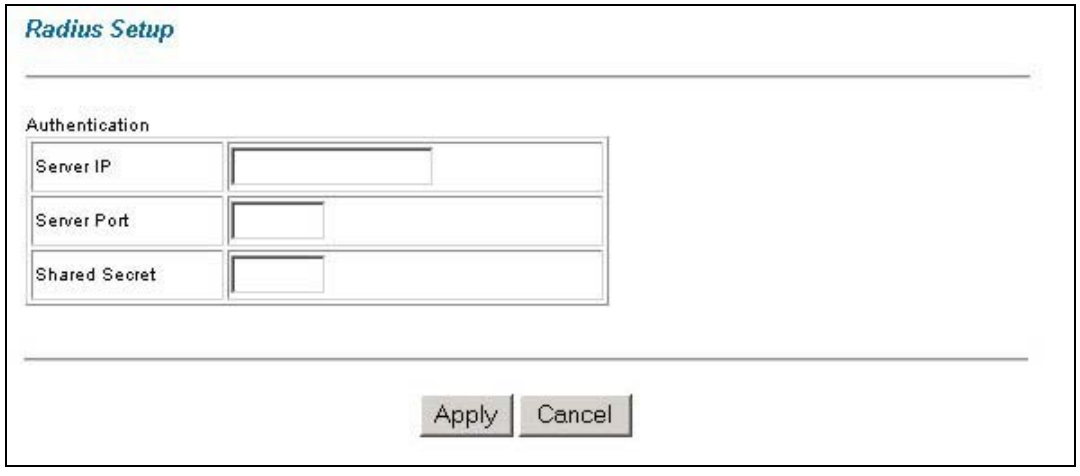

Figure 15-2 RADIUS Setup

Table 15-1 RADIUS Setup

FIELD	DESCRIPTION
Authentication	
Server IP	Enter the IP address of the external RADIUS server in dotted decimal notation.
Port	The default port of the RADIUS server for authentication is **1812**. You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Specify a password (up to 31 alphanumeric characters) as the key to be shared between the external RADIUS server and the switch. This key is not sent over the network. This key must be the same on the external RADIUS server and the switch.
Click **Apply** to save your changes back to the switch or click **Cancel** to begin configuring this screen afresh.	

Chapter 16 Logins

Configure up to four administrators using this screen

16.1 Introduction

Up to four people may administer the switch via web configurator at any one time. Configure passwords for each administrator in the menu.

It is highly recommended that you change the default password ("1234").

Click **Logins** from the navigation panel.

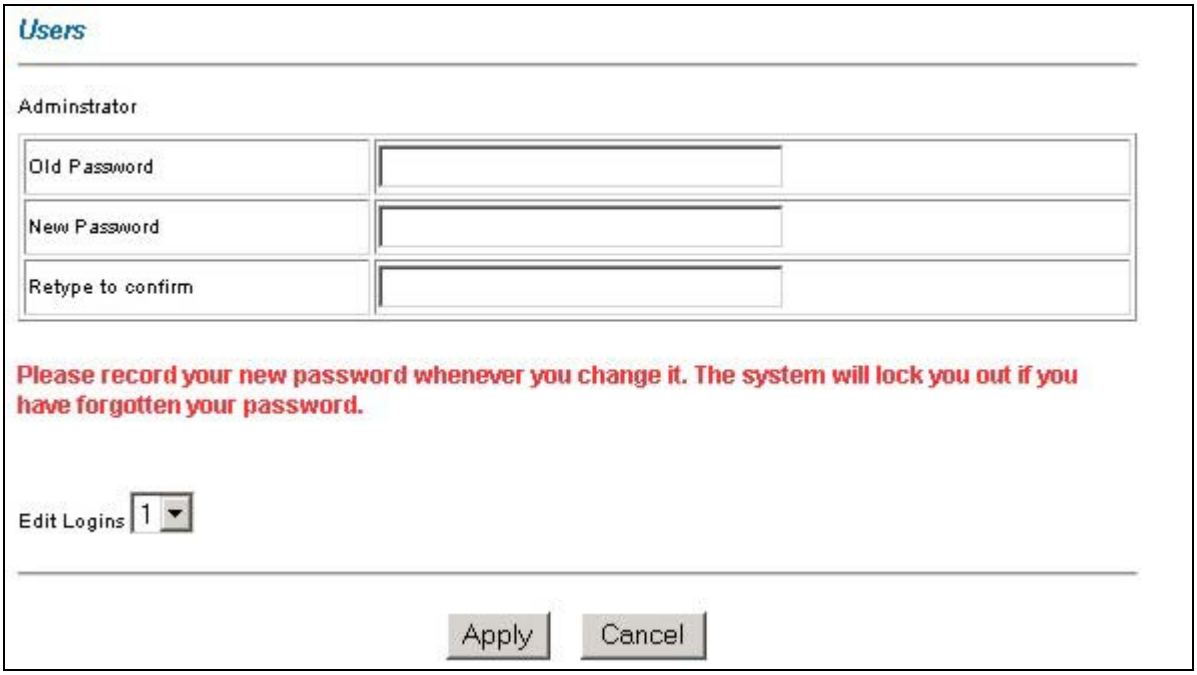

Figure 16-1 Logins

The following table describes the menu fields.

Table 16-1 Logins

FIELD	DESCRIPTION
Old Password	Type the existing system password ("1234" is the default password when shipped).
New Password	Enter your new system password.
Retype to confirm	Retype your new system password for confirmation
Edit Logins	You may configure passwords for up to four users from this drop-down list. Click on one of Login 1 to Login 4 and set a user name and password for each user as shown in the next screen and described in the previous three fields.
Click **Apply** to save your changes back to the switch or click **Cancel** to begin configuring this screen afresh.	

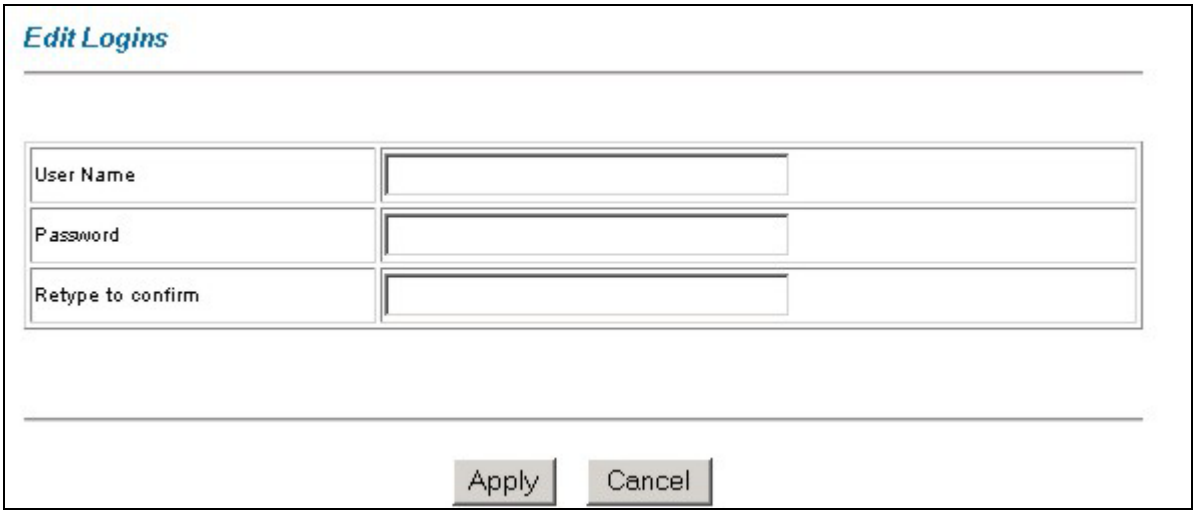

Figure 16-2 Edit Logins

Chapter 17 Maintenance

This chapter explains how to configure the maintenance screens. The links on the upper right of the Maintenance screen lead to different screens that let you maintain the firmware and configuration files.

17.1 Maintenance

Click **Maintenance** in the navigation panel to open the following screen.

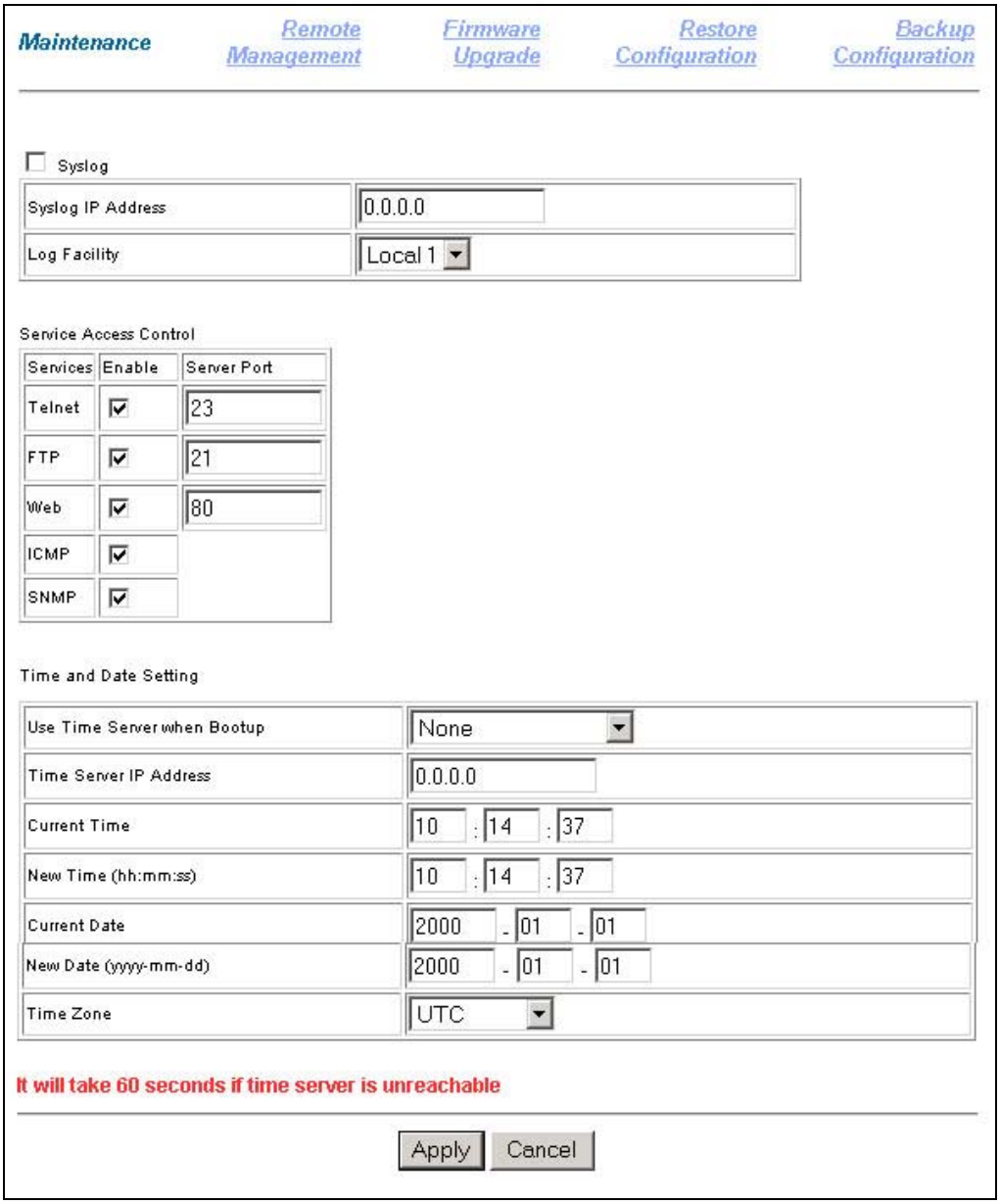

Figure 17-1 Maintenance

Table 17-1 Maintenance

LABEL	DESCRIPTION
Syslog	Select this check box to activate syslog (UNIX system logging) and then configure the UNIX syslog parameters described in the following fields.
Syslog IP Address	Enter the IP address of the syslog server.
Log Facility	Select one of seven different options from the drop-down list box. The log facility allows you to log the message to different files in the server. Please refer to your UNIX manual for more details.
Service Access Control	Service Access Control allows you to decide what services you may use to access the ES-3024. You may also change the default service port and configure “trusted computer(s)” for each service in the **Remote Management** screen (see later in this guide).
Services	Services you may use to access the ES-3024 are listed here.
Enable	Select the **Enable** check boxes for the corresponding services that you want to allow to access the ES-3024.
Server Port	For Telnet, FTP or web services, you may change the default service port by typing the new port number in the **Server Port** field. If you change the default port number then you will have to let people (who wish to use the service) know the new port number for that service.
Time and Date Setting	**Time and Date Setting** allows you to set the time manually or get the current time and date from an external server when you turn on your switch. The real time is then displayed in the switch logs.
Use Time Server When Bootup	Enter the time service protocol that your timeserver sends when you turn on the switch. Not all timeservers support all protocols, so you may have to use trial and error to find a protocol that works. The main differences between them are the time format. **Daytime (RFC 867)** format is day/month/year/time zone of the server. **Time (RFC-868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. **NTP (RFC-1305)** is similar to Time (RFC-868). **None** is the default value. Enter the time manually. Each time you turn on the switch, the time and date will be reset to 2000-1-1 0:0.
Time Server IP Address	Enter the IP address (or URL if you configure a domain name server in the IP Setup screen) of your timeserver. The switch searches for the timeserver for up to 60 seconds. If you select a timeserver that is unreachable, then this screen will appear locked for 60 seconds. Please wait.
Current Time	This field displays the time you open this menu (or refresh the menu).
New Time (hh:min:ss)	Enter the new time in hour, minute and second format. The new time then appears in the **Current Time** field after you click **Apply**.
Current Date	This field displays the date you open this menu.
New Date (yyyy-mm-dd)	Enter the new date in year, month and day format. The new date then appears in the **Current Date** field after you click **Apply**.

Table 17-1 Maintenance

LABEL	DESCRIPTION
Time Zone	Select the time difference between UTC (Universal Time Coordinated, formerly known as GMT, Greenwich Mean Time) and your time zone from the drop-down list box.
Click **Apply** to save your changes back to the switch or click **Cancel** to begin configuring this screen afresh.	

17.2 Remote Management

Click **Remote Management** in the **Maintenance** screen to display the following screen.

A "secured client set" is a group of one or more "trusted computers" from which an administrator may use a service to manage the switch. Configure "trusted computer(s)" for each service in the **Remote Management** screen. Click **Maintenance** to return to the first **Maintenance** screen.

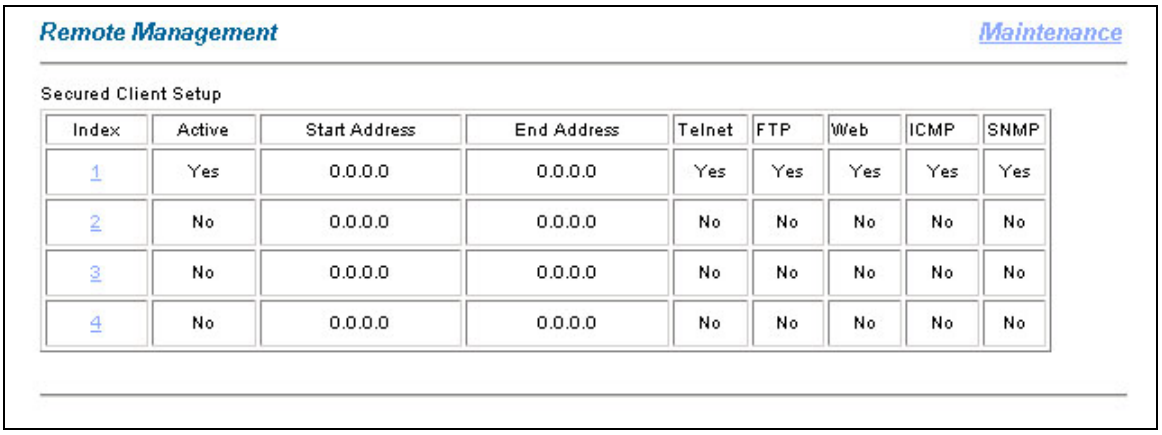

Figure 17-2 Remote Management

Table 17-2 Remote Management

FIELD	DESCRIPTION
Index	This is the client set index number. A "client set" is a group of one or more "trusted computers" from which an administrator may use a service to manage the switch.
Active	**Yes** indicates the client set is active and **No** indicates that it is not active.
Start Address	The default value for a start and end address is 0.0.0.0, which means you don't care which host is trying to use a service/protocol.
End Address	This field displays the end IP address in a range of client IP addresses that may use the service(s) defined in the next field.
Telnet/FTP/Web/ICMP/SNMP	**Yes** means that the specified service/protocol is enabled for this client set. Similarly, **No** means it is not.
To edit a client set, click its client set index number.	

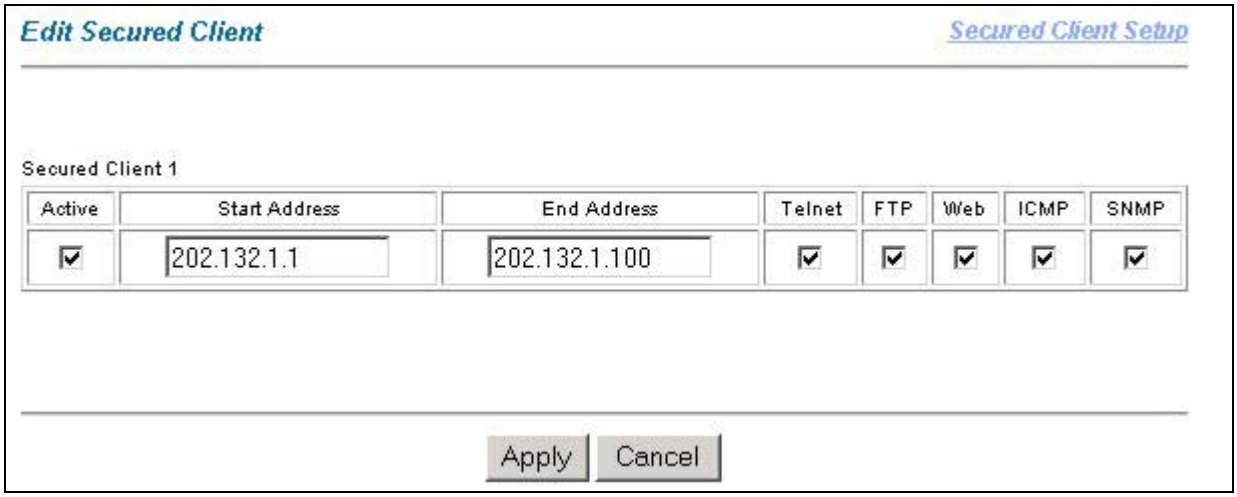

Figure 17-3 Edit Secured Client

Table 17-3 Edit Secured Client

LABEL	DESCRIPTION
Active	Select this check box to activate this secured client set. Clear the check box if you wish to temporarily disable the set without deleting it.
Start Address End Address	Configure the IP address range of trusted computers fro which you can manage this switch. The switch checks if the client IP address of a computer requesting a service or protocol matches the range set here. The switch immediately disconnects the session if it does not match.
Telnet/FTP/Web/ICMP/SNMP	Select services that may be used for managing the switch from the specified trusted computers.
Click **Apply** to save your changes back to the switch or click **Cancel** to begin configuring this screen afresh.	

Chapter 18 Firmware and Configuration File Maintenance

This chapter shows you how to manage configuration files and upgrade firmware.

18.1 Firmware Upgrade

Click **Firmware Upgrade** in the **Maintenance** screen if you want to upgrade your switch firmware. See the **Statistics** screen to verify your current firmware version number. Make sure you have downloaded (and unzipped) the correct model firmware and version to your computer before uploading to the device.

Be sure to upload correct model firmware as uploading the wrong model firmware may damage your device.

Click **Maintenance** to go back to the first **Maintenance** screen when done.

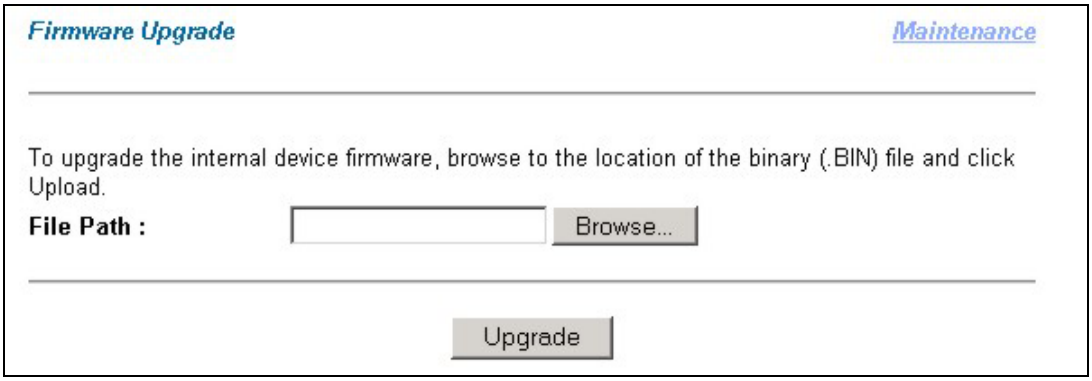
Firmware Upgrade
Maintenance
To upgrade the internal device firmware, browse to the location of the binary (.BIN) file and click Upload.
File Path :
Browse...
Upgrade

Figure 18-1 Firmware Upgrade

Type the path and file name of the firmware file you wish to upload to the switch in the **File Path** text box or click **Browse** to display the **Choose File** screen from which you can locate it. After you have specified the file, click **Upload**.

18.2 Restore a Configuration File

Backing up your switch configurations allows you to create various “snap shots” of your device from which you may restore at a later date. Restore a previously saved configuration from your computer to the switch using this screen. Click **Restore Configuration** in the **Maintenance** screen.

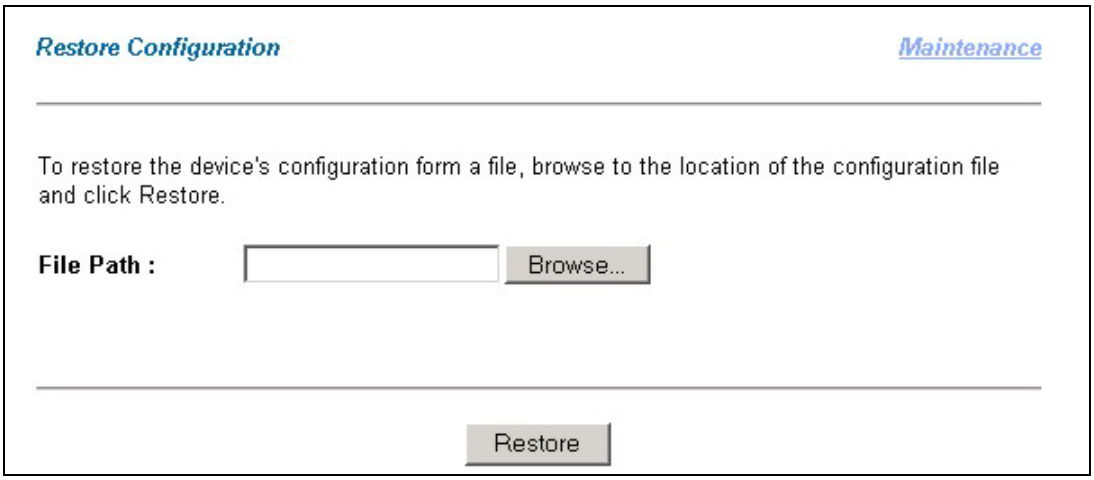
Restore Configuration
Maintenance
To restore the device's configuration form a file, browse to the location of the configuration file and click Restore.
File Path :
Browse...
Restore

Figure 18-2 Restore Configuration

Type the path and file name of the configuration file you wish to restore in the **File Path** text box or click **Browse** to display the **Choose File** screen (below) from which you can locate it. After you have specified the file, click **Restore**. "rom-0" is the name of the configuration file on the switch, so your backup configuration file is automatically renamed when you restore using this screen.

18.3 Back Up a Configuration File

Back up your current switch configuration to a computer using this screen. Click **Backup** in the **Maintenance** screen.

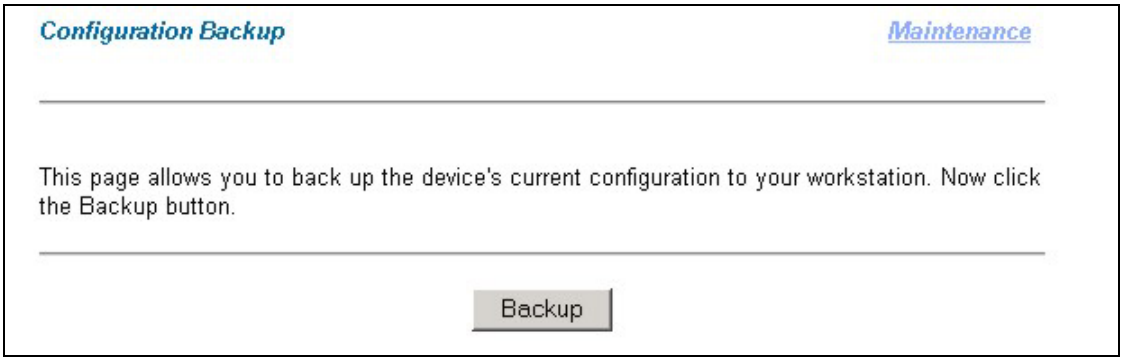
Configuration Backup
Maintenance
This page allows you to back up the device's current configuration to your workstation. Now click the Backup button.
Backup

Figure 18-3 Backup Configuration

Click **Backup**.

Choose **Save this file to disk** to display the **Save As** screen.

Choose a location to save the file on your computer from the **Save in** drop-down list box and type a descriptive name for it in the **File name** list box. Click **Save** to save the configuration file to your computer.

18.4 Command Line FTP

This section shows some examples of uploading to or downloading files from the switch using FTP commands. First, understand the filename conventions.

18.4.1 Filename Conventions

The configuration file (often called the romfile or rom-0) contains the factory default settings in the screens such as password, switch setup, IP Setup, etc. It arrives from ZyXEL with a “rom” filename extension. Once you have customized the switch's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (ZyXEL Network Operating System sometimes referred to as the “ras” file) is the system firmware and has a “bin” filename extension.

Table 18-1 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	Rom-0	*.rom	This is the configuration filename on the switch. Uploading the rom-0 file replaces the entire ROM file system, including your switch configurations, system-related data (including the default password), the error log and the trace log.
Firmware	Ras	*.bin	This is the generic name for the ZyNOS firmware on the switch.

Example FTP Commands

```
ftp> put firmware.bin ras
```

This is a sample FTP session showing the transfer of the computer file " firmware.bin" to the switch .

```
ftp> get rom-0 config.cfg
```

This is a sample FTP session saving the current configuration to a file called “config.cfg” on your computer.

If your (T)FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the switch only recognizes “rom-0” and “ras”. Be sure you keep unaltered copies of both files for later use.

Be sure to upload correct model firmware as uploading the wrong model firmware may damage your device.

18.4.2 FTP Command Line Procedure

Step 1. Launch the FTP client on your computer.

Step 2. Enter “open”, followed by a space and the IP address of your switch.

Step 3. Press [ENTER] when prompted for a username.

Step 4. Enter your password as requested (the default is “1234”).

Step 5. Enter “bin” to set transfer mode to binary.

Step 6. Use “put” to transfer files from the computer to the switch, for example, “put firmware.bin ras” transfers the firmware on your computer (firmware.bin) to the switch and renames it “ras”. Similarly, “put config.rom rom-0” transfers the configuration file on your computer (config.rom) to the switch and

renames it “rom-0”. Likewise “get rom-0 config.rom” transfers the configuration file on the switch to your computer and renames it “config.rom.” See earlier in this chapter for more information on filename conventions.

Step 7. Enter “quit” to exit the ftp prompt.

18.4.3 GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

Table 18-2 General Commands for GUI-based FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Anonymous. This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option. Normal. The server requires a unique User ID and Password to login.
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode. Configuration and firmware files should be transferred in binary mode.
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

18.4.4 FTP over WAN Restrictions

FTP over WAN will not work when:

- Telnet service is disabled in **Secured Client Sets**.
- The IP address(es) in the **Secured Client Sets** menu does not match the client IP address. If it does not match, the switch will disconnect the Telnet session immediately.

Chapter 19 Statistics

This chapter explains the Advanced Management Statistics screens.

19.1 Introduction to Statistics

The web configurator provides statistics screens to allow you to see how much traffic the switch is handling and how it is handling it.

Click **Statistics** in the navigation panel to open this screen. Use this screen to view general information and to access other screens with more detailed statistical information.

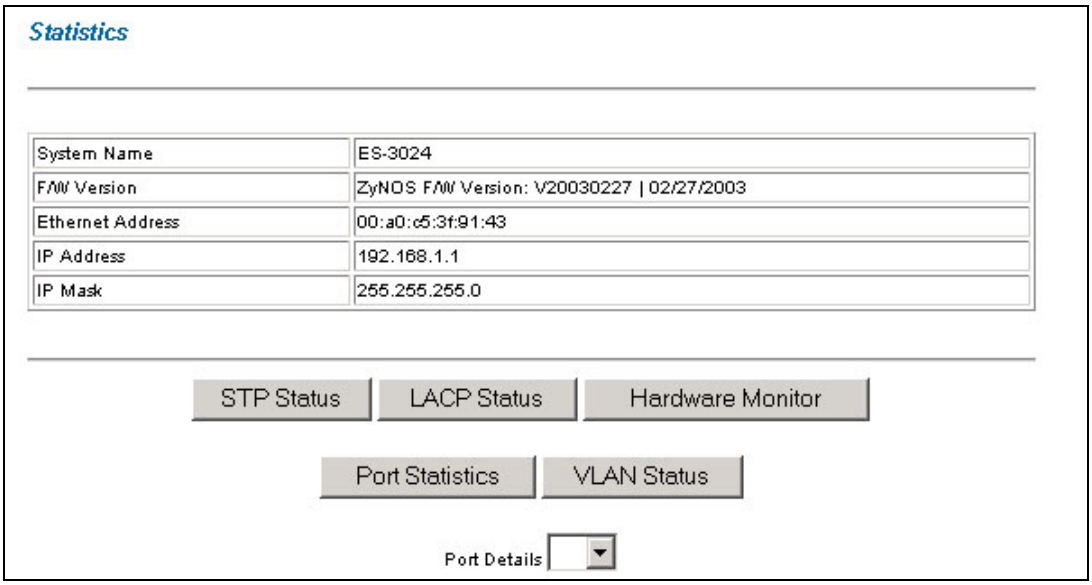

Figure 19-1 Statistics

Table 19-1 Statistics

LABEL	DESCRIPTION
System Name	This field displays the switch 's model name.
F/W Version	This field displays the version number of the switch 's current firmware including the date created.
Ethernet Address	This field refers to the Ethernet MAC (Media Access Control) address of the switch.
IP Address	This is the IP address of the switch in dotted decimal notation.
IP Mask	This shows the IP subnet mask of the switch.
STP Status	Click this button to display Spanning Tree Protocol statistics.

Table 19-1 Statistics

LABEL	DESCRIPTION
LACP Status	Click this button to display Link Aggregation Control Protocol (LACP) trunking statistics.
Hardware Monitor	Click this button to display hardware (fan, temperature, and voltage) statistics.
Port Statistics	Click this button to display statistics on all ports.
VLAN Status	Click this button to display 802.1Q VLAN statistics.
Port Details	Select a port from the drop-down list box to display individual port statistics.

19.1.1 STP Status

Click **STP Status** in the **Statistics** screen to open this screen. Use this screen to view Spanning Tree Protocol information about the root bridge and this switch (this switch may be the root bridge). See the ***Switch Setup*** chapter for more information on STP.

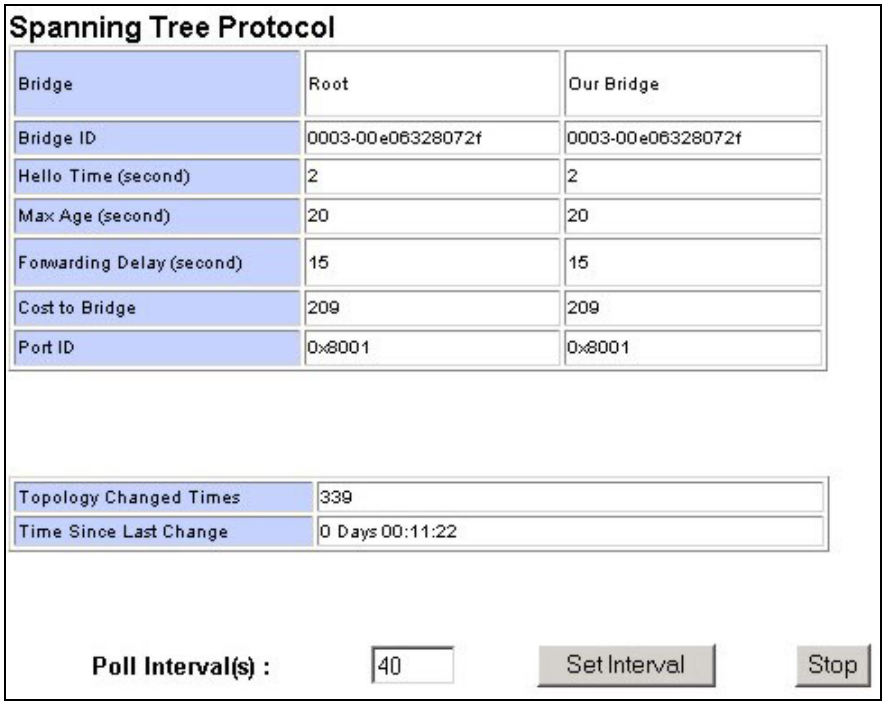

Figure 19-2 STP Statistics

Table 19-2 STP Statistics

LABEL	DESCRIPTION
Bridge	**Root** refers to the base of the spanning tree (the root bridge). **Our Bridge** is this switch. This switch may also be the root bridge.

Table 19-2 STP Statistics

LABEL	DESCRIPTION
Bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address. This ID is the same for **Root** and **Our Bridge** if the switch is the root switch.
Hello Time (second)	This is the time interval (in seconds) at which the root switch transmits a configuration message. The root bridge determines **Hello Time**, **Max Age** and **Forwarding Delay.**
Max Age (second)	This is the maximum time (in seconds) a switch can wait without receiving a configuration message before attempting to reconfigure.
Forwarding Delay (second)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding).
Cost to Bridge	This is the path cost from the root port on this switch to the root switch.
Port ID	This is the priority and number of the port on the switch through which this switch must communicate with the root of the Spanning Tree.
Topology Changed Times	This is the number of times the spanning tree has been reconfigured.
Time Since Last Change	This is the time since the spanning tree was last reconfigured.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Set Interval**.
Stop	Click **Stop** to halt STP statistic polling.

19.1.2 LACP Status

Click **LACP Status** in the **Statistics** screen to open this screen. Use this screen to view port trunking. See the ***Switch Setup*** chapter for more information on LACP.

LACP aggregation ID consists of the following information:

AGGREGATOR ID:

[(0000,00-00-00-00-00-00,0000,00,0000)] [(0000,00-00-00-00-00-00,0000,00,0000)]

Local switch				
0000	00-00-00-00-00	0000	00	0000
System priority	Local switch MAC address	Key	Port Priority[1]	Port Number[1]

Peer switch				
0000	00-00-00-00-00	0000	00	0000
System priority	MAC address	Key	Port Priority[1]	Port Number[1]

Figure 19-3 Aggregator ID:

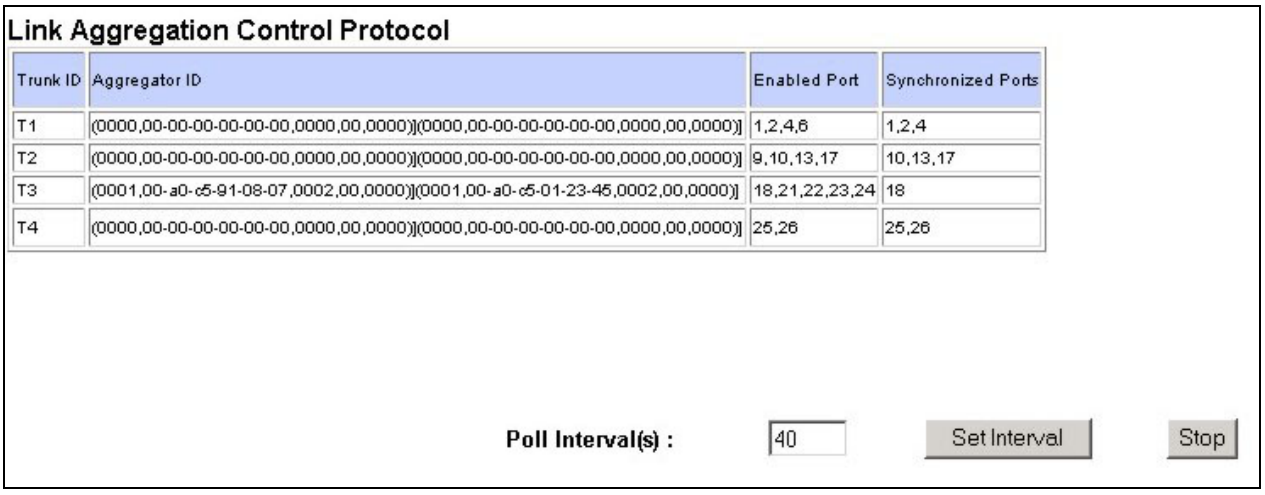

Figure 19-4 LACP Status

Table 19-3 LACP Statistics

LABEL	DESCRIPTION
Trunk ID	The trunk ID identifies the trunk group, that is, one logical link containing multiple ports – see the *Trunk Setup chapter* for more in formation on trunk groups.
Aggregator ID	See *Figure 19-3* for more detailed information on this field.
Enabled Port	These are the ports you have configured in the **Trunk Setup** screen to be in the trunk group.
Synchronized Ports	These are the ports that are currently transmitting data as one logical link in this trunk group.

[1] This is "0" as it is the aggregator ID for the trunk group, not the individual port.

Table 19-3 LACP Statistics

LABEL	DESCRIPTION
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Set Interval**.
Stop	Click **Stop** to halt statistic polling.

19.1.3 Hardware Monitor

Click **Hardware Monitor** in the **Statistics** screen to open this screen. Use the hardware performance statistics in this screen for hardware troubleshooting.

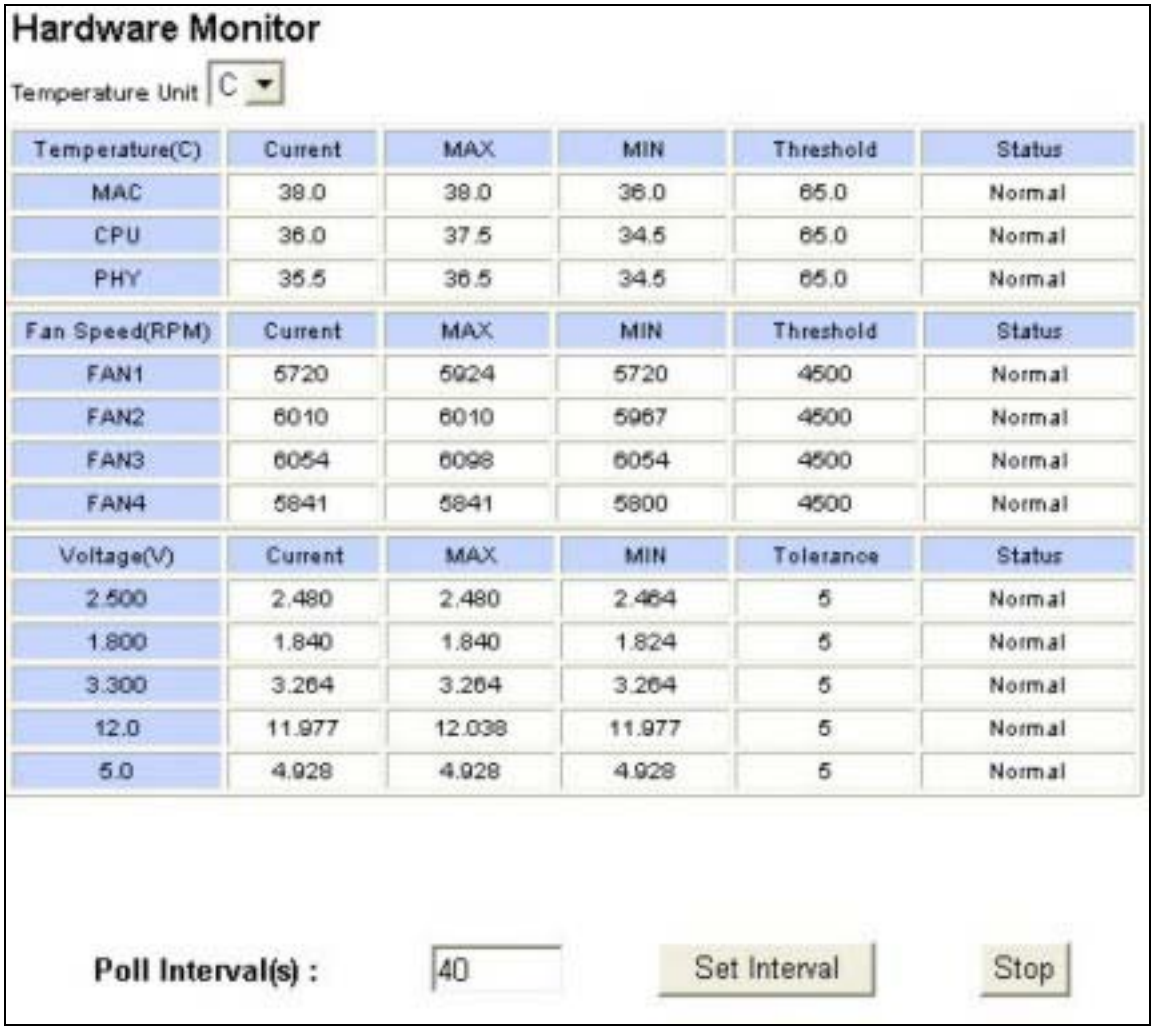
Hardware Monitor
Temperature Unit C
Temperature(C) Current MAX MIN Threshold Status
MAC 38.0 38.0 36.0 65.0 Normal
CPU 36.0 37.5 34.5 65.0 Normal
PHY 35.5 36.5 34.5 65.0 Normal
Fan Speed(RPM) Current MAX MIN Threshold Status
FAN1 5720 5924 5720 4500 Normal
FAN2 6010 6010 5967 4500 Normal
FAN3 6054 6098 6054 4500 Normal
FAN4 5841 5841 5800 4500 Normal
Voltage(V) Current MAX MIN Tolerance Status
2.500 2.480 2.480 2.464 5 Normal
1.800 1.840 1.840 1.824 5 Normal
3.300 3.264 3.264 3.264 5 Normal
12.0 11.977 12.038 11.977 5 Normal
5.0 4.928 4.928 4.928 5 Normal
Poll Interval(s) : 40 Set Interval Stop

Figure 19-5 Hardware Monitor

Table 19-4 Hardware Monitor

LABEL	DESCRIPTION
Temperature Unit (C)	The switch has temperature sensors that are capable of detecting and reporting if the temperature rises above the threshold. You may choose the temperature unit (Centigrade or Fahrenheit) in this field. **MAC**, **CPU** and **PHY** refer to the location of the temperature sensors on the switch printed circuit board.
Current	This shows the current temperature in degrees centigrade at this sensor.
Max	This field displays the maximum temperature measured at this sensor.
Min	This field displays the minimum temperature measured at this sensor.
Threshold	This field displays the upper temperature limit at this sensor.
Status	This field displays **Norma**l for temperatures below the threshold and **Error** for those above.
Fan speed (RPM)	A properly functioning fan is an essential component (along with a sufficiently ventilated, cool operating environment) in order for the device to stay within the temperature threshold. Each fan has a sensor that is capable of detecting and reporting if the fan speed falls below the threshold shown.
Current	This field displays this fan's current speed in Revolutions Per Minute (RPM).
Max	This field displays this fan's maximum speed measured in Revolutions Per Minute (RPM).
Min	This field displays this fan's minimum speed measured in Revolutions Per Minute (RPM). "<41" is displayed for speeds too small to measure (under 2000 RPM).
Threshold	This field displays the minimum speed at which a normal fan should work.
Status	**Normal** indicates that this fan is functioning above the minimum speed. **Error** indicates that this fan is functioning below the minimum speed.
Voltage(V)	The power supply for each voltage has a sensor that is capable of detecting and reporting if the voltage falls out of the tolerance range.
Current	This is the current voltage reading.
Max	This field displays the maximum voltage measured at this point.
Min	This field displays the minimum voltage measured at this point.
Tolerance	A tolerance of plus-minus five percent is the acceptable deviation from the nominal voltage.
Status	**Normal** indicates that the voltage is within an acceptable operating range at this point; otherwise **Error** is displayed.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Set Interval**.
Stop	Click **Stop** to halt statistic polling.

19.1.4 VLAN Status

Click **VLAN Status** in the **Statistics** screen to open this screen. Use this screen to check status and membership data about the card's IEEE 802.1Q VLANs.

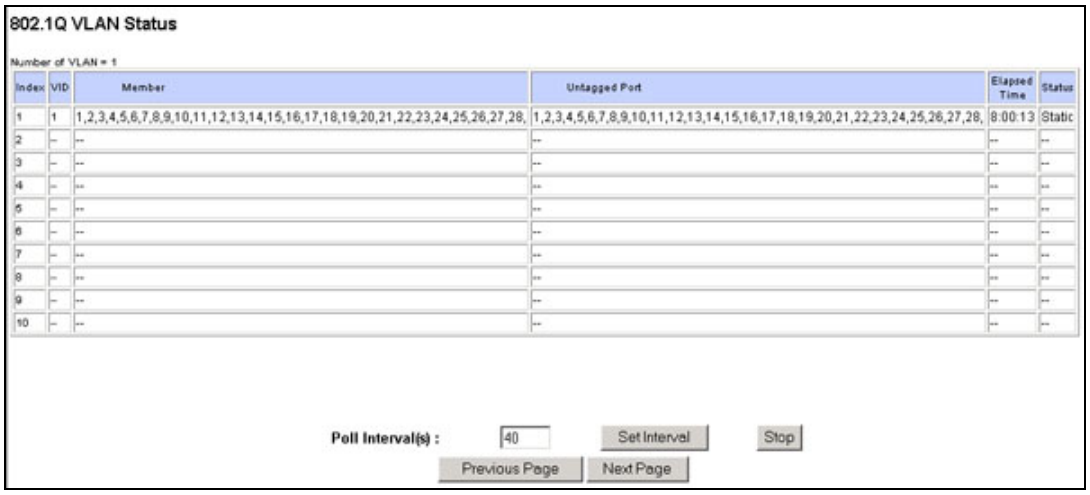

Figure 19-6 802.1Q VLAN Status

Table 19-5 802.1Q VLAN Status

LABEL	DESCRIPTION
Number of VLAN	This is the number of VLANs configured on the switch.
Index	This is the VLAN index number.
VID	This is the VLAN identification number that was configured in the **VLAN Setup** screen.
Member	Ports that have been added to this VLAN are listed here in numerical order.
Untagged Port	Untagged ports that have been added to this VLAN are listed here in numerical order.
Elapsed Time	This field shows how long it has been since a normal VLAN was registered or a static VLAN was set up.
Status	This field shows how this VLAN was added to the switch; dynamically using GVRP or statically, that is, added as a permanent entry.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Set Interval**.
Stop	Click **Stop** to halt polling statistics.
Previous/Next Page	Click one of these buttons to show the previous/next screen if all status information cannot be seen in one screen.

19.1.5 Port Statistics

Click **Port Statistics** in the **Statistics** screen to open this screen. Use this screen to check status and performance data about the switch's ports.

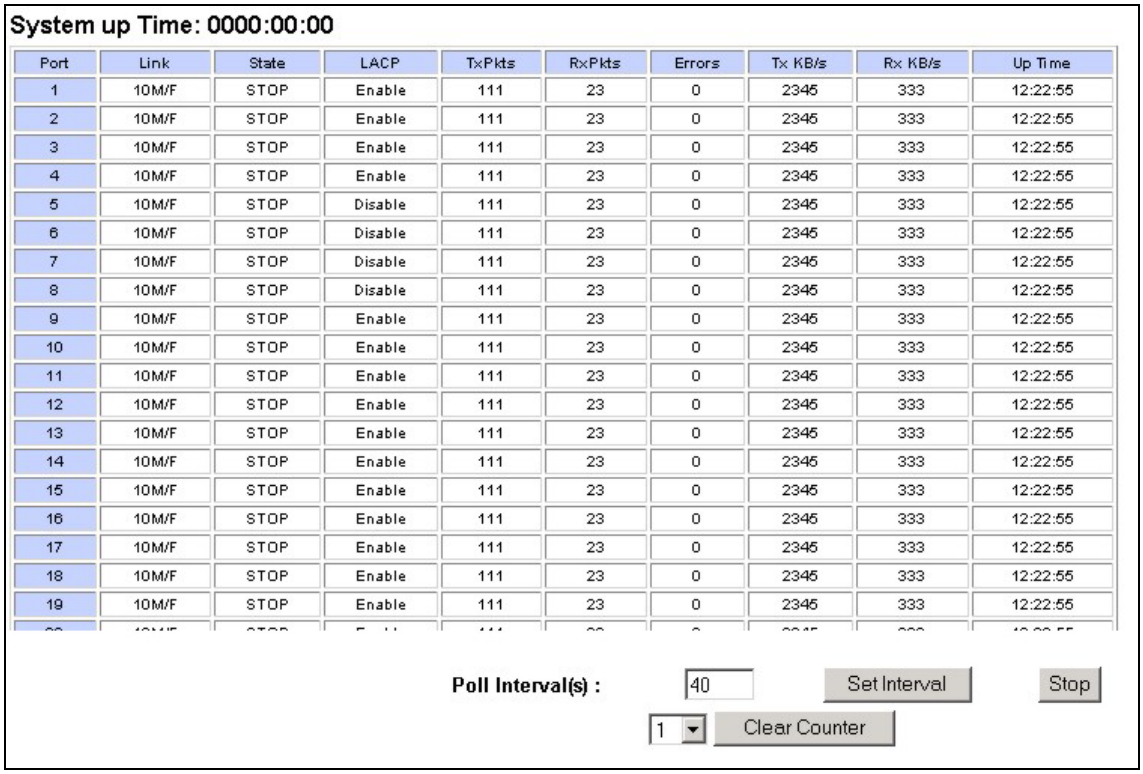

Figure 19-7 Port Statistics

Table 19-6 Port Statistics

LABEL	DESCRIPTION
System up Time	This field shows how long the system has been running since the last time it was started.
Port	This identifies the Ethernet port.
Link	This field displays the speed (either **10M** for 10Mbps, **100M** for 100Mbps or another value depending on the uplink module being used) and the duplex (**F** for full duplex or **H** for half).
State	This field displays the STP state of the port. See the ***Switch Setup*** chapter for details on STP states.
LACP	This fields displays whether LACP has been enabled on the port.
TxPkts	This field shows the number of transmitted frames on this port.
RxPkts	This field shows the number of received frames on this port.
Errors	This field shows the number of received errors on this port.

Table 19-6 Port Statistics

LABEL	DESCRIPTION
Tx KB/s	This field shows the number of kilobytes per second transmitted on this port.
Rx KB/s	This field shows the number of kilobytes per second received on this port.
Up Time	This field shows the total amount of time in hours, minutes and seconds the port has been up.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Set Interval**.
Stop	Click **Stop** to halt system statistic polling.
Clear Counter	Choose a port from the drop-down list box and then click **Clear Counter** to erase the recorded statistical information for that port.

19.1.6 Port Details

Select a port from the **Port Details** drop-down list box in the **Statistics** screen to display individual port statistics. Use this screen to check status and detailed performance data about an individual port on the card.

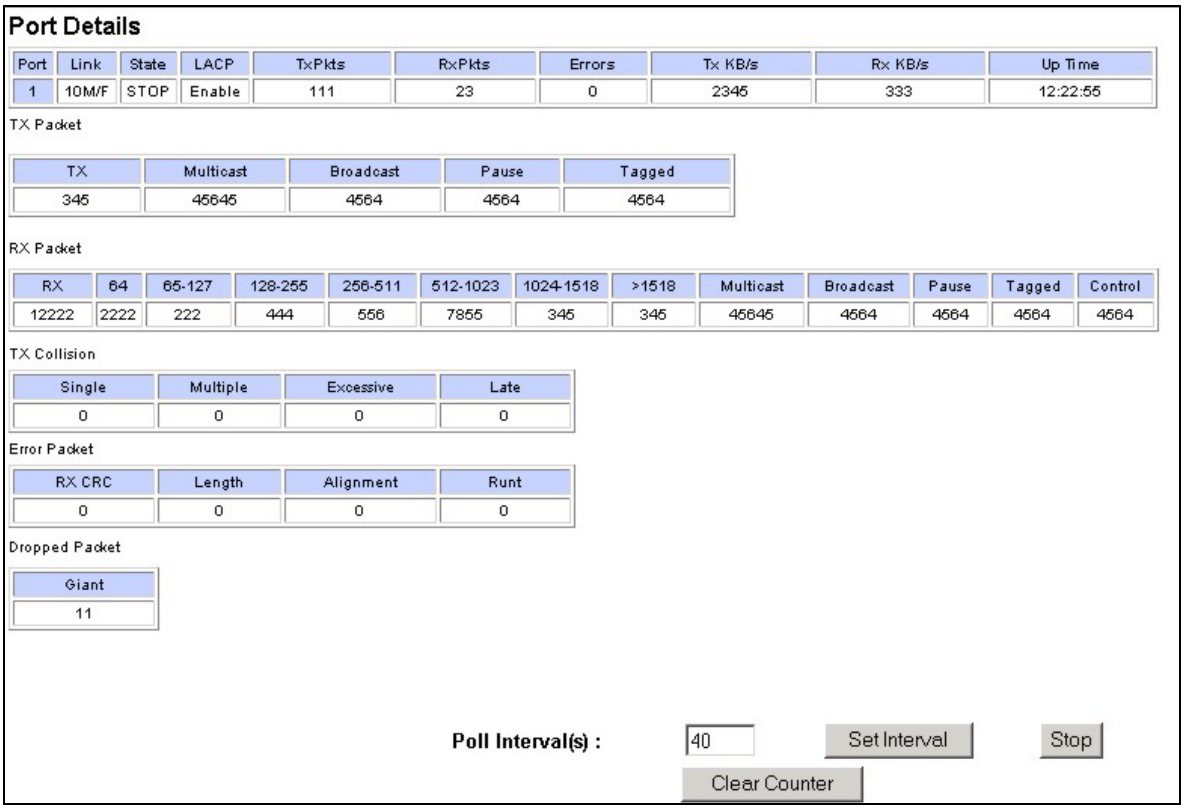
Port Details
Port Link State LACP TxPkts RxPkts Errors Tx KB/s Rx KB/s Up Time
1 10M/F STOP Enable 111 23 0 2345 333 12:22:55
TX Packet
TX Multicast Broadcast Pause Tagged
345 45645 4564 4564 4564
RX Packet
RX 64 65-127 128-255 256-511 512-1023 1024-1518 >1518 Multicast Broadcast Pause Tagged Control
12222 2222 222 444 556 7855 345 345 45645 4564 4564 4564 4564
TX Collision
Single Multiple Excessive Late
0 0 0 0
Error Packet
RX CRC Length Alignment Runt
0 0 0 0
Dropped Packet
Giant
11
Poll Interval(s) :
40
Set Interval
Stop
Clear Counter

Figure 19-8 Port Details

Table 19-7 Port Details

LABEL	DESCRIPTION
Port	This refers to the port number.
Link	This field shows whether the Ethernet connection is down, and the speed/duplex mode.
State	This field shows the training state of the ports. The states are FORWARDING (forwarding), which means the link is functioning normally or STOP (the port is stopped to break a loop or duplicate path).
LACP	This field shows if LACP is enabled on this port or not.
TxPkts	This field shows the number of transmitted frames on this port
RxPkts	This field shows the number of received frames on this port
Errors	This field shows the number of received errors on this port.
Tx KB/s	This field shows the number kilobytes per second transmitted on this port.
Rx KB/s	This field shows the number of kilobytes per second received on this port.
Up Time	This field shows the total amount of time the connection has been up.
Tx Packet	The following fields display detailed information about frames transmitted.
TX	This field shows the number of good frames (unicast, multicast and broadcast) transmitted.
Multicast	This field shows the number of good multicast frames transmitted.
Broadcast	This field shows the number of good broadcast frames transmitted.
Pause	This field shows the number of 802.3x Pause frames transmitted.
Tagged	This field shows the number of frames with VLAN tags transmitted.
Rx Packet	The following fields display detailed information about frames received.
RX	This field shows the number of good frames (unicast, multicast and broadcast) received.
64	This field shows the number of frames (including bad frames) received that were 64 octets in length.
65-127	This field shows the number of frames (including bad frames) received that were between 65 and 127 octets in length.
128-255	This field shows the number of frames (including bad frames) received that were between 128 and 255 octets in length.
256-511	This field shows the number of frames (including bad frames) received that were between 256 and 511 octets in length.
512-1023	This field shows the number of frames (including bad frames) received that were between 512 and 1023 octets in length.
1024-1518	This field shows the number of frames (including bad frames) received that were between 1024

Table 19-7 Port Details

LABEL	DESCRIPTION
	and 1518 octets in length.
>1518	This field shows the number of frames (including bad frames) transmitted that were greater than 1518 octets in length.
Multicast	This field shows the number of good multicast frames received.
Broadcast	This field shows the number of good broadcast frames received.
Pause	This field shows the number of 802.3x Pause frames received.
Tagged	This field shows the number of frames with VLAN tags received.
Control	This field shows the number of control received (including those with CRC error) but it does not include the 802.3x Pause frames.
TX Collision	The following fields display information on collisions while transmitting.
Single	This is a count of successfully transmitted frames for which transmission is inhibited by exactly one collision.
Multiple	This is a count of successfully transmitted frames for which transmission was inhibited by more than one collision.
Excessive	This is a count of frames for which transmission failed due to excessive collisions. Excessive collision is defined as the number of maximum collisions before the retransmission count is reset.
Late	This is the number of times a late collision is detected, that is, after 512 bits of the frame have already been transmitted.
Error Packet	The following fields display detailed information about frames received that were in error.
RX CRC	This field shows the number of frames received with CRC (Cyclic Redundant Check) error(s).
Length	This field shows the number of frames received with a length that was out of range.
Alignment	This field shows the number of frames received of proper size but with CRC error(s) and a non-integral number of octets.
Runt	This field shows the number of frames received that were too short (shorter than 64 octets), including the ones with CRC errors.
Dropped Packet	The following filed indicates why frames were dropped.
Giant	This field shows the number of frames dropped because they were bigger than the maximum frame size.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Set Interval**.
Stop	Click **Stop** to stop port statistic polling.
Clear Counter	Click this button to erase the recorded statistical information for this port.

Chapter 20 Diagnostic

This chapter explains the Diagnostic screens.

20.1 Diagnostic

Click **Diagnostic** in the navigation panel to open this screen. Use this general diagnostic screen to check system logs, reset the system or ping IP addresses. Click the Ethernet port link in this screen to diagnose an Ethernet port.

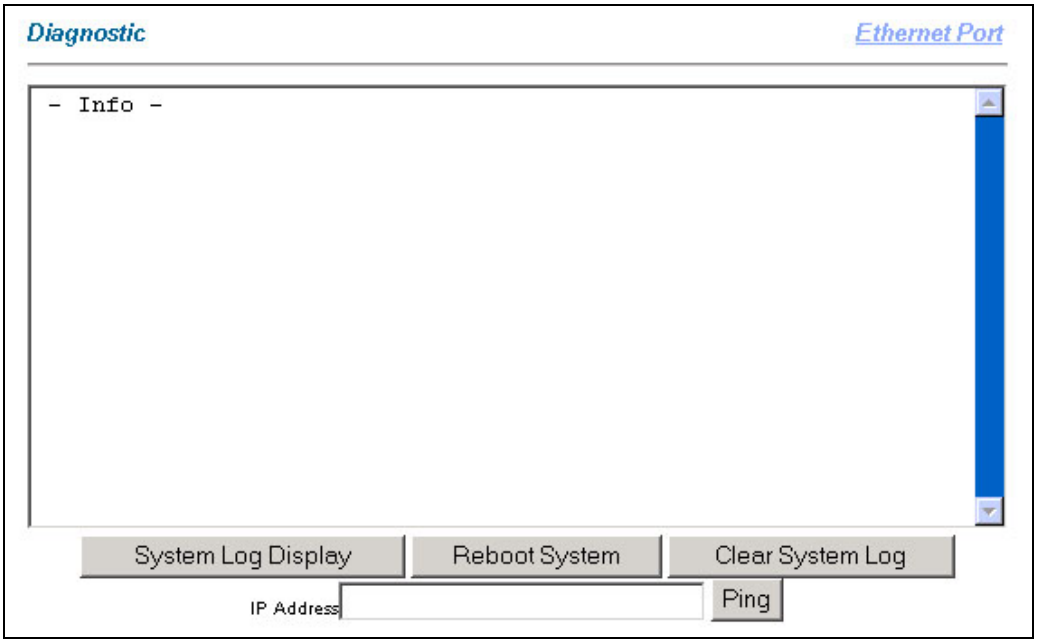

Figure 20-1 Diagnostic Screen

Table 20-1 Diagnostic Screen

LABEL	DESCRIPTION
System Log Display	Click this button to display a log of events in the multi-line text box.
Reboot System	Click this button to restart the switch. A warning dialog box displays asking if you're sure. Click **OK** to proceed.
Clear System Log	Click this button to clear the log of events in the multi-line text box.
IP Address	Type the IP address of a device that you want to ping in order to test a connection.
Ping	Click this button to have the device ping the IP address (in the field to the left) 5 times.

Part VI

Commands

This part gives information on commands for the ES-3024.

Chapter 21
Commands Introduction

This chapter introduces line commands and gives a summary of commands available.

21.1 Command Line Interface Overview

In addition to the web configurator, you can use line commands to configure the switch. It is recommended that you use the web configurator for everyday management of the switch and that you use line commands for advanced switch diagnosis and troubleshooting. If you have problems with your switch, customer support may request that you issue some of these commands to assist them in troubleshooting.

You can use the "config save" command to save tagged IEEE 802.1Q VLAN and STP commands in non-volatile memory (Flash) but all other line command configurations are saved in volatile memory (DRAM) only, so are not effective after you restart the switch!

Telnet to the switch or connect a computer to the console port and use terminal emulation software configured to the following parameters:

- VT100 terminal emulation
- No parity, 8 data bits, 1 stop bit
- 9600 bps
- No flow control

21.1.1 Command Conventions

The system uses a one-level command structure. You must type the full command every time, as follows.

```
192.168.1.1> <command>
```

For instance, the following example shows how to enable GVRP.

```
192.168.1.1> sys sw gvrp enable
```

The conventions for typing in most CI commands are shown next.

```
command <interface|device> subcommand [parameter]
command subcommand [parameter]
```

21.1.2 Command Syntax Conventions

1. Command keywords are in `courier new` font.
2. The | symbol means "or".
3. Required fields in a command are enclosed in angle brackets <>. Use the following command to turn the system monitor on or off.

```
sys monitor enable <on/off>
```

4. Optional fields in a command are enclosed in square brackets `[]`, for example, year, month and day are optional in the following command. This command just displays the date if you don't specify the year, month and day parameters.

```
sys date [year month day]
```

5. Commands can be abbreviated to the smallest unique string that differentiates the command. For example the "system date" command could be abbreviated to "s d".

6. Type "help" or "?" to display a list of valid commands or type a command followed with "help" or "?" to display a list of associated subcommands.

21.2 Command Summary

The following tables are summaries of the commands available in the ES-3024 together with a brief description of each command. See the related section in the *User's Guide* for more background information.

Table 21-1 command summary

COMMAND			DESCRIPTION
sys			
	adjtime		Retrieves the date and time from the time server specified in the web configurator.
	date	[year month day]	Sets or displays the system's current date.
	edit		Edits the system preset text file such as autoexec.net.
	feature		Displays a list of the device's major features.
	hostname	[hostname]	Sets or displays the system name.
	log		
		clear	Clears the error log.
		disp	Shows the error log.
		online [on|off]	Enables/disables the error log to be displayed on screen.
	stdio	[minute]	Sets or displays the management terminal idle timeout value.
	time	[hour [min [sec]]]	Sets or displays the system time.
	trcdisp	parse, brief, disp	Sets the level of detail that should be displayed. Use "parse" to display the most detail and "disp" to display the least.
	trclog		

Table 21-1 command summary

COMMAND			DESCRIPTION
		switch [on|off]	Enables/disables/ the system trace log or shows whether it's on or off.
		online [on|off]	Enables/disables the trace log onscreen display (for example in the telnet management window).
		level [level]	Sets the level (1-10) of trace logs (1 shows the least) to display.
		type <bitmap>	Uses hexadecimal characters to set the type of trace logs to record.
		disp	Shows the trace log.
		clear	Erases the trace log.
		call	Shows call events.
		encapmask [mask]	Shows which type of encapsulation the trace log records or sets it if you specify the encapsulation's hexadecimal character.
	trcpacket		
		create <entry> <size>	Creates a packet trace buffer.
		destroy	Removes the packet trace buffer.
		channel <name> [none|incoming|outgoing|bothway]	Sets the packet trace direction for a given channel.
		string [on|off]	Enables/disables the sending of a log to the trace packet buffer when configuration changes are made or displays the current setting.
		switch [on|off]	Enables/disables packet trace or displays the current setting.
		disp	Displays the trace packets.
		udp	Sends the trace packets to another system using UDP.
		udp switch [on|off]	Enables/disables the sending of the trace packets to another system using UDP or displays the current setting.
		udp addr <addr>	Sets the target IP address for sending trace packets using UDP.
		udp port <port>	Sets the UDP port (should match that of the target IP address) for sending trace packets using UDP.
		parse [[start_idx], end_idx]	Displays detailed packet details of the packet range specified.

Table 21-1 command summary

COMMAND			DESCRIPTION
		brief	Displays a brief listing of packet contents.
	version		Displays the RAS code and driver versions.
	view	view <filename>	Displays the specified text file.
	wdog		
		switch [on|off]	Turns the watchdog firmware protection feature on or off.
		cnt [value]	Sets (0-34463) or displays the current watchdog count (in 1.6 sec units).
	monitor	status	Displays the status of the hardware monitor.
		show	Displays the hardware monitor's statistics.
		vlimit <idx> <high> <low>	Sets the maximum (<high>) or minimum (<low>) voltage at the specified point (<idx>).
		tlimit <idx> <limit>	Sets the maximum (<limit>) temperature at the specified point (<idx>).
		flimit <bank> <idx> <limit>	Sets the maximum (<limit>) fan revs per minute (RPM) at the specified fan (<idx>) in the specified bank (<bank>). A "bank" delineates a set of fans.
		fanmask <bank> [<mask>]	Sets the fan detection mask in the specified bank (<bank>). Use the mask to disable monitoring of a fan.
		vclear	Clears the voltage statistics.
		tclear	Clears the temperature statistics.
		fclear	Clears the fan statistics.
		clear	Clears the hardware monitor statistics.
		enable [<on/off>]	Enables or disables the hardware monitor.
		test	Tests the hardware monitor chip.
	ixe2424	lbt intlbt <port|All> [count]	ixe2424 refers to the switch chip. Performs an internal loop back test on a specified port or all ports.
		lbt extlbt <port|All> [count]	Performs an external loop back test on a specified port or all ports.

Table 21-1 command summary

COMMAND			DESCRIPTION
		pktcnt <port>	Display port statistic counter
		pktcntclear <port>	Reset port statistic counter
		port <portID> <enable | disable> <Speed> <FlowCtrl>	Port setup
		phyread <portID> [<phyAddr>]	Read PHY register
		phywrite <portID> <phyAddr> <data>	Write PHY register
		dbm mac cnt [port]	Display number in L2 DBM
		Dbm mac list [port]	Display entries in L2 DBM
		Dbm mac search <MAC> <VID>	Search the MAC/VID learnt on which port.
		log level [0-4]	Sets the log level. Logs displayed consist of critical, error, warning, debug and informational messages in order of severity. Log level “4” displays all messages; log level “0” just displays critical messages.
		log switch on/off	Outputs messages to the console or telnet screen.
		log list	Lists all IXE log modules.
		Log module <module_id> <on/off	Enable / disable log on specific IXE module
		log switch < on|off >	Log all modules to tracelog. (Current display to console directly)
		memdum <start_addr> <length>	Displays the switch chip’s memory map for the block specified.
		wreg <addr> <value>	Writes to a register.
		rreg <addr>	Reads from a register.
		show_int_count	Displays the interrupt counter.
		clear_int_count	Resets the interrupt counter.
	socket		Displays the system socket’s ID #, type, control block address (PCB), IP address and port number of peer device connected to the socket (Remote Socket) and task control block (Owner).
	cpu	display	Displays the CPU’s utilization.
	snmp	getCommunity [<community>]	Sets or displays the SNMP GetRequest community.

Table 21-1 command summary

COMMAND			DESCRIPTION
		setCommunity [<community>]	Sets or displays the SNMP SetRequest community.
		trustedHost [<hostt>]	Sets or displays the SNMP trusted host.
		trapCommunity [<community>]	Sets or displays the SNMP Trap community.
		trapDest [<destination>]	Sets or displays the SNMP trap server.
		disp	Shows SNMP settings.
	server	access <telnet|ftp|web|icmp> <enable/disable>	Enables or disables a service.
		port <telnet|ftp|web> <portNo>	Sets a port for a service.
		secIP setEntry <index> <start-addr> <end-addr> [[TELNET] [FTP] [WEB] [ICMP]]	Sets a secured entry.
		secIP active <index>	Turns on a secured entry.
		secIP inactive <index>	Turns off a secured entry.
		sec IP disp	Shows the secured entries.
		disp	Shows the device's service port numbers and access control settings.
exit			Ends the console or telnet session.
ip			
	address	[addr]	Displays the host IP address.
	alias	<iface>	Sets an alias for the specified interface.
	aliasdis	<0|1>	Disables/enables the alias for the specified interface.
	arp	status <iface>	Displays an interface's IP Address Resolution Protocol status.
	httpd	debug [on|off]	Enables or disables the HTTP debug flag.
	icmp		
		status	Displays the ICMP statistics counter.
		discovery <iface> [on|off]	Sets the ICMP router discovery flag.
	ifconfig	[iface] [ipaddr] [broadcast <addr> |mtu <value>|dynamic]	Configures a network interface.

Table 21-1 command summary

COMMAND			DESCRIPTION
	ping	<hostid>	Pings a remote host.
	route		
		status [if]	Displays the routing table.
		add <dest_addr|default>[/<bits>] <gateway> [<metric>]	Adds a route.
		addiface <dest_addr|default> [/<bits>] <gateway> [<metric>]	Adds an entry to the routing table for the specified interface.
		addprivate <dest_addr|default> [/<bits>] <gateway> [<metric>]	Adds a private route.
		drop <host addr> [/<bits>]	Drops a route.
	status		Displays IP statistic counters.
	udp	status	Displays the UDP status.
	tcp		
		ceiling [value]	Sets the TCP maximum round trip time.
		floor [value]	Sets the TCP minimum round trip time.
		irtt [value]	Sets the TCP default initial round trip time.
		kick <tcb>	Drops the TCP connection of the specified TCP Control Block.
		limit [value]	Sets a TCP output window limit.
		mss [value]	Inputs the TCP Maximum Segment Size.
		reset <tcb>	Resets the TCP connection of the specified TCP Control Block.
		rtt <tcb> <value>	Sets the round trip time for the TCP control block.
		status [tcb] [<interval>]	Displays the TCP statistic counters.
		syndata [on|off]	Turns on/off the option to send data with the SYN packet.
		trace [on|off]	Turns on/off the trace for debugging.
	telnet	<host> [port]	Telnets to the specified host.
		support	Shows if TFTP is supported.
		stats	Displays the TFTP status.

Table 21-1 command summary

COMMAND			DESCRIPTION
	traceroute	<host> [ttl] [wait] [queries]	Sends ICMP packets to trace the route of a remote host.
	igmpsnoop		
		status	Displays the IGMP group table.
		querier	Displays the port number of the incoming port that received the latest IGMP querier.
		enable	Turns on IGMP snooping.
		disable	Turns off IGMP snooping.
config	save		This command stores tagged IEEE 802.1Q VLAN and STP configurations only in nonvolatile memory. All other command configurations are lost when you restart the switch.

The following commands are system switch commands; all are preceded with `sys sw` .

COMMAND			DESCRIPTION
garp	status		Shows the GARP timer status.
	timer	<join timer(ms)><leave timer(ms)><leave all timer<ms>	Sets the GARP timer's Join Timer, Leave Timer and Leave All Timer.
gvrp	status		Shows whether GVRP is enabled or not.
	enable		Enables GVRP.
	disable		Disables GVRP.
qos	defpri	<port> [<0..7>]	Sets the default ingress User Priority for a port.
	map	<0..7> [<queue>]	Maps a User Priority to a Traffic Class.
vlan1q			All "sys sw vlan1q" commands relate to IEEE 802.1Q Tagged VLAN configuration. Use "config save" to save your configuration changes.
	port	status <port>	Shows a port's VLAN information.
		defaultvid <port><vid>	Sets the default VLAN ID of a port.
		accept <port> <all|tagged>	Sets the type of frames that a port accepts.

COMMAND			DESCRIPTION
		gvrp <port> <enable|disable>	Enables/disables GVRP on the specified port.
	svlan	cpu <vlan id>	Sets the VLAN ID of the management VLAN (CPU).
		setentry<name><vid><port><adctl> <tagctl>	Applies a static VLAN (name, admin control tag, tag control) to a port.
		delentry <vid>	Deletes the specified (VID) static VLAN.
		active <vid>	Turns on the specified static VLAN.
		inactive <vid>	Turns off the specified static VLAN.
		list	Displays a table of static VLANs.
	vlan	list <all|vid|start_vid end_vid>	Shows the specified IEEE 802.1Q Tagged VLAN table.
	status		Shows the IEEE 802.1Q tagged status.
driver	config		Shows the switch's settings.
	count	disp	Shows the switch Network Driver Interface Specifications (NDIS) level counters (CPU interface).
		clear	Clears the switch NDIS level counters (CPU interface).
rstp			All "sys sw rstp" commands relate to rapid STP configuration. Refer to IEEE Std 802.1w. Use "config save" to save your configuration changes.
	bridge		
		enable	Enables RSTP.
		disable	Disables RSTP.
		priority <priority>	Sets the system priority.
		maxage <max age>	Sets the max age timer
		hellotime <hello time>	Sets the hello timer.
		forwarddelat <forward delay time>	Sets the forward delay time
		version <stp:0|rstp:2>	Displays/enables the STP mode; STP or RSTP. RSTP is the default used when configuring STP via web configurator.
	port		
		enable <port_no>	Enables RSTP on this port.
		disable <port_no>	Disables RSTP on this port.

COMMAND			DESCRIPTION
		pathcost <port_no>	Displays the specified port's path cost.
		priority <port_no>	Displays the specified port's priority.
		edgeport <port_no>	Displays if this port is an edge port.
		p2plink <port_no>	Displays whether the specified port can connect to one bridge or multiple bridges.
		mcheck <port_no>	Enables the Port Protocol Migration state machine (Disabled, Blocking, Listening, Learning, Forwarding) on the specified port.
lacp			Refer to IEEE 802.3ad for more information on link aggregation control protocol.
	agg		Displays ports trunked using LACP.
	port		
		enable <port_no>	Enables LACP on the specified port.
		disable <port_no>	Disables LACP on the specified port.
		status <port_no>	Displays whether LACP is enabled on the specified port.
		actoradm activity [port_no] [0:passive 1:active]	Allows/disallows the specified local port to engage in trunking.
		actoradm display [port_no]	Shows whether the specified local port is engaged in trunking.
		actoradm key [port_no][key]	Shows the specified local port LACP key.
		actoradm priority [port_no] [priority]	Shows the specified local port LACP priority.
		actoradm timeout [port_no] [0:long_timeout|1:short_timeout]	Enables a short or long timeout on the specified local port.
		status	Displays LACP status on all ports.
		keymgnt [on|off]	Turns LACP key management on or off.
		syspriority <priority>	Sets the LACP system priority. The switch with the lowest priority becomes the LACP "server".
dot1x			"sys sw dot1x" commands relate to IEEE 802.1X security.

COMMAND			DESCRIPTION
	enable		Enables 802.1X security on the switch.
	disable		Disables 802.1X security on the switch.
	status		Shows switch 802.1X security status.
	port		
		enable <port_no>	Enables 802.1X security on the specified port.
		disable <port_no>	Disables 802.1X security on the specified port.
		reauth <port_no> <on|off>	Turns re-authentication on or off on the specified port.
		reauthperiod <port_no><value>	Configures how often the specified port should be re-authenticated.
		status <port_no>	Displays 802.1X security status on the specified port.
	set		
		auth <profile | radius>	Sets whether an external RADIUS server or the internal switch user database performs authentication.
		portcontrol<port-no><auto |auth | unauth>	Sets how the specified port should be authenticated.
	radius		
		server <ip>	Sets the external RADIUS server IP address.
		secret <secret>	Sets the external RADIUS server password.
		port <port>	Sets the external RADIUS server port number.
		show	Displays the external RADIUS server settings.
	profile		Internal switch user database. Information in this database is flushed on restarting the switch.
		add <username> <passwd>	Creates a username and password profile in the internal switch user database.
		delete <idx>	Deletes a username and password profile in the internal switch user database.

COMMAND			DESCRIPTION
		list	Lists all profiles in the internal switch user database.
class			A class is the basic rule parameters for a bandwidth control, port mirror or port filter rule.
	display		Displays run-time bandwidth control, port mirror and port filter rule status.
	l2set	<src port> <src mac> <src vid><dest port><dest mac> <dest vid>	Sets source/destination port, MAC address and VLAN group information.
	del	<class id>	A class is automatically created when you create a bandwidth control, port mirror or port filter rule. This command deletes the specified class.
bmstorm			These commands relate to broadcast storm control.
	disable		Clears current run-time settings
	type	<type>	Specifies the type of frames to limit in the switch; broadcast, multicast or both.
	basis	<type>	Specifies whether frames are limited in the switch on a per-packet or per-Byte basis.
	display	[index]	Displays broadcast storm control ports' settings
	interval	[value]	Sets/displays the monitor interval.
	set	<port><threshold><direction>	Specifies the packet threshold and direction (ingress/egress) on the specified port.
	del	<index>	Disables broadcast storm control on this port.
mac	static		Displays static MAC addresses.
		disable	Clears current run-time static MAC address settings
		display [port]	Displays current run-time static MAC addresses on the specified port.
		set<port><mac addr.><vid>	Configures a static MAC address on the specified port.

COMMAND			DESCRIPTION
.		del<port><mac addr.><vid>	Deletes a static MAC address on the specified port.
filter			The following commands relate to port filters. Port filtering means sifting traffic from one or all ports to one or all ports based on the source and/or destination MAC addresses and VLAN group.
	disable		Clears current run-time filters.
	display		Displays current run-time filter status.
	set	<src port><src mac><src vid><dest port><dest mac><dest vid>	Creates a filter rule using source/destination port, MAC address and VLAN group information. “*” means “any”.
mirror			The following commands relate to port mirrors. Port mirroring is copying traffic from one or all ports to another or all ports for external analysis.
	disable		Clears current run-time port mirror settings.
	display		Displays current run-time port mirror settings.
	set	<src port><src mac><src vid><dest port><dest mac><dest vid>	Creates a mirror rule using source/destination port, MAC address and VLAN group information. “*” means “any”.
		<input|output|both>	Sets the direction of mirrored traffic.
	port	<port>	Sets the mirror port (the port traffic is copied to for analysis).
bw			The following commands relate to bandwidth control rules. Bandwidth control means defining a maximum allowable bandwidth for traffic flows from specified source(s) to specified destination(s).
	disable		Clears current run-time bandwidth control rules.
	display		Displays current run-time bandwidth control rules.

COMMAND			DESCRIPTION
	set	<src port><src mac><src vid><dest port><dest mac><dest vid><max bw>	Creates a bandwidth control rule using source/destination port, MAC address and VLAN group information. “*” means “any”.
trunk			The following commands relate to trunking. Trunking is the grouping of physical ports into one logical higher-capacity link.
	disable		Clears current run-time trunk settings.
	display		Displays current run-time trunk settings.
	set	<group><# ports>	Adds ports to a trunk group.
	del	<group>	Delete the specified trunk group.

Chapter 22
Command Examples

This chapter describes some commands in more detail.

22.1 Commonly Used Commands Overview

These are commands that you may use frequently in configuring and maintaining your switch. See the following chapter for IEEE 802.1Q Tagged VLAN commands.

22.2 Sys Commands

These are the commonly used commands that belong to the sys (system) group of commands.

22.2.1 Log Disp Command

Syntax:

```
ras> sys log disp
```

This command displays the system error log.

An example is shown next.

```
ras> sys log disp
   1 Wed Feb 12 15:27:45 2003 PP1d  ERROR unknown variable
   6 Wed Feb 12 15:34:42 2003 PP13  INFO  SMT Password pass
   9 Wed Feb 12 16:16:46 2003 PP13  INFO  SMT Password pass
  11 Wed Feb 12 16:26:06 2003 PP1d  ERROR unknown variable
  12 Wed Feb 12 16:31:18 2003 PP13  INFO  SMT Password pass
  14 Wed Feb 12 16:42:20 2003 PP13  INFO  SMT Password pass
  16 Wed Feb 12 16:55:39 2003 PP13  INFO  SMT Password pass
  18 Wed Feb 12 17:19:30 2003 PP13  INFO  SMT Password pass
  20 Wed Feb 12 17:43:31 2003 PP13  INFO  SMT Password pass
  22 Wed Feb 12 17:45:48 2003 PP1d  ERROR unknown variable
  23 Thu Feb 13 09:08:09 2003 PP14  ERROR Last errorlog repeat 54 Times
  26 Thu Feb 13 09:23:53 2003 PP13  INFO  SMT Password pass
  28 Thu Feb 13 09:36:05 2003 PP13  INFO  SMT Password pass
  30 Thu Feb 13 09:52:48 2003 PP13  INFO  SMT Password pass
  34 Thu Feb 13 10:32:02 2003 PP13  INFO  SMT Password pass
  36 Thu Feb 13 11:51:02 2003 PP1f  INFO  adjtime task pause 1 day
  37 Thu Feb 13 12:06:22 2003 PP13  INFO  SMT Password pass
  39 Thu Feb 13 12:15:12 2003 PP13  INFO  SMT Password pass
  42 Thu Feb 13 16:17:25 2003 PP13  INFO  SMT Password pass
```

Figure 22-1 Log Disp Command Example

22.2.2 Log Clear Command

Syntax:

```
ras> sys log clear
```

This command clears the system error log.

If you clear a log (using the `log clear` command), you cannot view it again.

22.2.3 Version Command

Syntax:

```
ras> sys version
```

This command shows the RAS code, firmware version, system uptime and bootbase version.

An example is shown next.

```
ras> sys version

 ZyNOS version: V3.50(DS.0)b16 | 03/30/2003
 romRasSize: 1638380
 system up time:    29:15:35 (a0baac ticks)
 bootbase version: V1.02| 02/26/2003
```

Figure 22-2 Version Command Example

22.2.4 Monitor Status Command

Syntax:

```
ras> sys monitor status
```

This command shows the hardware monitor's status.

An example is shown next.

```
ras> sys monitor status
   Time      V0     V1     V2     V3     V4     T0    T1    T2   F10   F11
Err
or
---------- ------ ------ ------ ------ ------ ----- ----- ----- ----- ----- ---
-
----
   160200   2.512  1.856  3.312  4.999  4.999  35.0  33.5  29.5  2909  3013
0000
0000
```

Figure 22-3 Monitor Status Command Example

22.2.5 Enabling RSTP on the Stacking Module

Step 1. First enable RSTP

```
sys sw rstp bridge enable
```

Step 2. Then enable RSTP on the stacking port.

```
sys sw rstp port enable 27
```

```
sys sw rstp port enable 28
```

Step 3. Save the configuration

```
config save
```

Chapter 23
IEEE 802.1Q Tagged VLAN

This chapter describes the IEEE 802.1Q Tagged VLAN and associated commands. Use the "config save" command to save configuration changes.

23.1IEEE 802.1Q Tagged VLAN Overview

See the *VLAN Setup* chapter for more information on VLANs. There are two kinds of tagging:

1. Explicit Tagging

A VLAN identifier is added to the frame header that identifies the source VLAN.

2. Implicit Tagging

The MAC (Media Access Control) number, the port or other information is used to identify the source of a VLAN frame.

The IEEE 802.1Q Tagged VLAN uses both explicit and implicit tagging.

It is important for the switch to determine what devices are VLAN-aware and VLAN-unaware so that it can decide whether to forward a tagged frame (to a VLAN-aware device) or first strip the tag from a frame and then forward it (to a VLAN-unaware device).

23.2Filtering Databases

A filtering database stores and organizes VLAN registration information useful for switching frames to and from a switch. A filtering database consists of a static entries (Static VLAN or SVLAN table) and dynamic entries (Dynamic VLAN or DVLAN table).

23.2.1 Static Entries (SVLAN Table)

Static entry registration information is added, modified and removed by administrators only.

23.2.2 Dynamic Entries (DVLAN Table)

Dynamic entries are learned by the switch and cannot be created or updated by administrators. The switch learns this information by observing what port, source address and VLAN ID (or VID) is associated with a frame. Entries are added and deleted using GARP VLAN Registration Protocol (GVRP), where GARP is the Generic Attribute Registration Protocol.

23.3Configuring Tagged VLAN

The following procedure shows you how to configure tagged VLAN.

Step 1. Use the IEEE 802.1Q tagged VLAN commands to configure tagged VLAN for the switch.

- Use the `sys sw vlan1q svlan setentry` command to configure a VLAN ID for each port on the switch.
- Use the `sys sw vlan1q svlan active` command when you are finished configuring the VLAN (see the last step).
- Use the `sys sw vlan1q port defaultVID command` to set the VLAN ID you created for a port to that specific port in the PVID table.
- Use the `sys sw vlan1q svlan active` command to activate the VLAN IDs.

Example:

```
1.      ras> sys sw vlan1q setentry up1 2000 24 fixed tag
2.      ras> sys sw vlan1q port defaultVID 24 2000
3.      ras> sys sw vlan1q setentry up2 2001 25 fixed untag
4.      ras> sys sw vlan1q port defaultVID 25 2001
5.      ras> sys sw vlan1q svlan active 2000
        ras> sys sw vlan1q svlan active 2001
```

Figure 23-1 Tagged VLAN Configuration and Activation Example

Step 2. Configure your management VLAN.

- Use the `sys sw vlan1q svlan setentry` command to configure a VLAN ID (VID 3 in this example) for managing the switch (the “management” or “CPU” VLAN).
- Use the `sys sw vlan1q svlan active` command to activate the new management VLAN ID.

Example:

```
1.      ras> sys sw vlan1q setentry 3 24 fixed tag
2.      ras> sys sw vlan1q svlan active 3
```

Figure 23-2 CPU VLAN Configuration and Activation Example

Step 3. Perform the procedure below to complete the VLAN setup.

a. Telnet to the operational IP address of the switch.

b. Use the `sys sw vlan1q svlan cpu` command to set VID 3 as the management VLAN.

c. Use the `sys sw svlan delentry` command to remove the default VLAN ID (1).

Example:

```
1.      ras> sys sw vlan1q svlan cpu 3
2.      ras> sys sw vlan1q svlan delentry 1
```

Figure 23-3 Deleting Default VLAN Example

23.4IEEE VLAN1Q Tagged VLAN Configuration Commands

These `sw` (switch) commands allow you to configure and monitor the IEEE 802.1Q Tagged VLAN.

23.4.1 GARP Status Command

Syntax:

```
ras> sys sw garp status
```

This command shows the switch's GARP timer settings, including the join, leave and leave all timers.

An example is shown next.

```
ras> sys sw garp status
GARP Timer Status :
        Join Timer = 200 msec
        Leave Timer = 600 msec
        Leave All Timer = 10000 msec
```

Figure 23-4 GARP Status Command Example

23.4.2 GARP Timer Command

Syntax:

```
ras> sys sw garp timer timer <join timer(ms)> <leave timer(ms)>
<leave all timer<ms>
```

where

`<join timer (ms)>`	=	This sets the duration of the Join Period timer for GVRP in milliseconds. Each port has a Join Period timer. The allowed Join Time range is between 100 and 32767 milliseconds; the default is 200 milliseconds.
`<leave timer(ms)>`	=	This sets the duration of the Leave Period timer for GVRP in milliseconds. Each port has a single Leave Period timer. Leave Time must be two times larger than Join Timer; the default is 600 milliseconds.

<leave all timer<ms>=	This sets the duration of the Leave All Period timer for GVRP in milliseconds. Each port has a single Leave All Period timer. Leave All Timer must be larger than Leave Timer; the default is 10000 milliseconds.

This command sets the switch's GARP timer settings, including the join, leave and leave all timers.

Switches join VLANs by making a declaration. A declaration is made by issuing a Join message using GARP. Declarations are withdrawn by issuing a Leave message. A Leave All message terminates all registrations. GARP timers set declaration timeout values.

The following example sets the Join Timer to 300 milliseconds, the Leave Timer to 800 milliseconds and the Leave All Timer to 11000 milliseconds.

```
ras> sys sw garp timer 300 800 11000
```

Figure 23-5 GARP Timer Command Example

23.4.3 GVRP Status Command

Syntax:

```
ras> sys sw gvrp status
```

This command shows the switch's GVRP settings.

An example is shown next.

```
ras> sys sw gvrp status
GVRP control block status:
  gvrpEnable = 1
  gvrpPortEnable:
    OOOOOOOOOOOOOOOOOOOOOOOOXXXX
```

Figure 23-6 GARP Status Command Example

23.4.4 GVRP Enable Command

Syntax:

```
ras> sys sw gvrp enable
```

This command turns on GVRP in order to propagate VLAN information beyond the switch.

23.4.5 GVRP Disable Command

Syntax:

```
ras> sys sw gvrp disable
```

This command turns off GVRP so that the switch does not propagate VLAN information to other switches.

23.4.6 VLAN1Q Port Status Command

Syntax:

```
ras> sys sw vlan1q port status <port>
```

This command shows information about the specified port's VLAN settings.

The following example shows the settings for port 1.

```
ras> sys sw vlan1q port status 1
Port 2 VLAN Setup :
Default VLAN ID = 1
VLAN Acceptable Type = Tagged Only
GVRP = Enable
```

Figure 23-7 VLAN1Q Port Status Command Example

23.4.7 VLAN1Q Port Default VID Command

Syntax:

```
ras> sys sw vlan1q port defaultVID <port> <VID>
```

where

`<port>` = A port number

`<VID>` = The VLAN ID. Valid parameter range = [1 – 4094].

This command sets a default VLAN ID for all untagged packets that come in through the specified port.

The following example sets the default VID of port 1 to 2000.

```
ras> sys sw vlan1q port defaultVID 1 2000
```

Figure 23-8 VLAN1Q Port Default VID Command Example

23.4.8 VLAN1Q Port Accept Command

Syntax:

```
ras> sys sw vlan1q port accept <port> <all|tagged>
```

where

`<port>` = A port number

`<all|tagged>` = Specifies all Ethernet frames (tagged and untagged) or only tagged

`<all|tagged>` = Specifies all Ethernet frames (tagged and untagged) or only tagged Ethernet frames.

This command sets the specified port to accept all Ethernet frames or only those with an IEEE 802.1Q VLAN tag.

The following example sets port 2 to accept only tagged frames.

```
ras> sys sw vlan1q port accept 2 tagged
```

Figure 23-9 VLAN1Q Port Accept Command Example

23.4.9 VLAN1Q Port GVRP Command

Syntax:

```
ras> sys sw vlan1q port gvrp <port> <enable|disable>
```

where

`<port>` = A port number

`<enable|disable>` = Turn GVRP on or off.

This command turns GVRP on or off for the specified port.

The following example turns off GVRP for port 2.

```
ras> sys sw vlan1q port gvrp 2 disable
```

Figure 23-10 VLAN1Q Port GVRP Command Example

23.4.10 VLAN1Q SVLAN CPU Command

Syntax:

```
ras> sys sw vlan1q svlan cpu <VLAN ID>
```

where

`<VID>` = The VLAN ID. Valid parameter range = [1 – 4094].

This command sets the management VLAN (CPU). You can only use ports that are members of this management VLAN in order to manage the switch.

The following example sets VLAN ID 2 to be the CPU (management) VLAN.

```
ras> sys sw vlan1q svlan cpu 2
```

Figure 23-11 VLAN1Q Port GVRP Command Example

23.4.11 VLAN1Q SVLAN Setentry Command

Syntax:

```
ras> sys sw vlan1q svlan setentry <name> <VID> <port> <adctl>
<tagctl>
```

where

`<name>`	=	A name to identify the SVLAN entry.
`<VID>`	=	The VLAN ID [1 – 4094].
`<port>`	=	This is the switch port number.
`<adctl>`	=	This is the registrar administration control flag. Valid parameters = [`fixed`, `forbidden`, `normal`]. Select `fixed` to register a `<port #>` to the static VLAN table with `<vid>`. Select `normal` to confirm registration of the `<port #>` to the static VLAN table with `<vid>`. Select `forbidden` to block a `<port #>` from joining the static VLAN table with `<vid>`.
`<tagctl>`	=	This is the tag control flag. Valid parameters = [`tag`|`untag`]. Select `tag` to tag outgoing frames. Select `untag` to send outgoing frames without a tag.

This command adds or modifies an entry in the static VLAN table. Display your configuration by using the `sys sw vlan1q svlan list` command. An example of a configuration is shown next.

Modify a Static VLAN Table Example

The following is an example of how to modify a static VLAN table.

```
1.      ras> sys sw vlan1q svlan setentry  2000  1  fixed  tag
2.      ras> sys sw vlan1q svlan setentry  2001  2  fixed  tag
```

Figure 23-12 Modifying the Static VLAN Example

Forwarding Process Example

Tagged Frames

Step 1. First the switch checks the VLAN ID (VID) of tagged frames or assigns temporary VIDs to untagged frames (see 23.4.7).

Step 2. The switch then checks the VID in a frame's tag against the SVLAN table.

Step 3. The switch notes what the SVLAN table says (that is, the SVLAN tells the switch whether or not to forward a frame and if the forwarded frames should have tags).

Step 4. Then the switch applies the port filter to finish the forwarding decision. This means that frames may be dropped even if the SVLAN says to forward them. Frames might also be dropped if they are sent to a CPE (customer premises equipment) DSL device that does not accept tagged frames.

Untagged Frames

Step 1. An untagged frame comes in from the LAN.

Step 2. The switch checks the PVID table and assigns a temporary VID of 1.

Step 3. The switch ignores the port from which the frame came, because the switch does not send a frame to the port from which it came. The switch also does not forward frames to "forbidden" ports.

Step 4. If after looking at the SVLAN, the switch does not have any ports to which it will send the frame, it won't check the port filter.

23.4.12 VLAN1Q SVLAN Delentry Command

Syntax:

```
ras> sys sw vlan1q svlan delentry <VID>
```

where

<VID> = The VLAN ID [1 – 4094].

This command deletes the specified VLAN ID entry from the static VLAN table

The following example deletes entry 2 in the static VLAN table.

```
ras> sys sw vlan1q svlan delentry 2
```

Figure 23-13 VLAN1Q SVLAN Delentry Command Example

23.5 VLAN1Q SVLAN Active Command

Syntax:

```
ras> sys sw vlan1q svlan active <VID>
```

This command enables the specified VLAN ID in the SVLAN (Static VLAN) table.

23.6 VLAN1Q SVLAN Inactive Command

Syntax:

```
ras> sys sw vlan1q svlan inactive <VID>
```

This command disables the specified VLAN ID in the SVLAN (Static VLAN) table.

23.7 VLAN1Q SVLAN List Command

Syntax:

```
ras> sys sw vlan1q svlan list
```

This command shows the IEEE 802.1Q Tagged SVLAN (Static VLAN) table.

An example is shown next.

For the `AdCtl` section of the last column, "-" is a port set to normal, "x" is a forbidden port and "F" is a fixed port.

For the `TagCtl` section of the last column, "T" is a tagged port, "U" is an untagged port.

```
ras> sys sw vlan1q svlan list
802.1Q VLAN Static Entry:
idx. Name         VID  Active   AdCtl / TagCtl
---- ------------ ---- -------- ------------------------
   0            1    1  active  ------------------------FFFF
                                 TTTTTTTTTTTTTTTTTTTTTTTTUUUU
```

Figure 23-14 VLAN1Q SVLAN List Command

23.8 VLAN1Q VLAN List Command

Syntax:

```
ras> sys sw vlan1q vlan list <all|VID|start_VID|end_VID>
```

where

`<all|VID|start_VID|end_VID>=`	Specify either all of the VLAN entries (`all`), a single VLAN ID (`VID`) or a range of VLAN IDs starting from a certain VID (`start_VID`) or a range of VLAN Ids ending at a specific VID (`end_VID`).

This command shows the current IEEE 802.1Q Tagged VLAN table or a specific part of it.

An example is shown next.

For the `EgressPort` section of the last column, "E" is an egress port for this VLAN, "-" is not an egress port for this VLAN.

The `UntaggedPort` section of the last column displays "-" for a tagged port and "U" for an untagged port.

```
ras> sys sw vlan1q vlan list all
   No.   VID  ElapsedTime  Status  EgressPort/UntaggedPort
  ------ ---- -----------  ------  --------------------------------
    1)     1     51:30:02  Static  ----E|EEE--|-----|-EEEE|EEEEE|EEE
                                   -----|-----|-----|-----|----U|UUU
```

Figure 23-15 VLAN1Q SVLAN List Command

23.8.1 VLAN Status Command

Syntax:

```
ras> sys sw vlan1q vlan status
```

This command displays the current configuration of the IEEE 802.1Q VLAN.

See the following example shows the default VLAN settings. The default VLAN allows all ports to connect to each other and sets them to send untagged packets.

```
ras> sys sw vlan1q status
802.1Q VLAN Setup :
 GVRP = Enable
 Managament VLAN ID = 1
```

Figure 23-16 VLAN1Q Status Command Example

Part VII

Appendices and Index

This part contains appendices of advanced background feature information and an Index.

Appendix A
Product Specifications

These are the ES-3024 product specifications.

Chart 1 General Product Specifications

Standards	IEEE802.3 10BASE-T Ethernet (twisted-pair copper) IEEE802.3u 100BASE-TX Fast Ethernet (twisted-pair copper) ANSI/IEEE802.3 Auto-negotiation IEEE802.3x Flow Control IEEE802.1p Priority Queues IEEE802.1q VLAN IEEE802.1d Spanning Tree IEEE 802.1x Authentication IEEE 802.3 ad Trunking IEEE 802.1w Rapid reconfiguration
Protocol	CSMA/CD
Interface	24 10/100BASE-T Ethernet ports Two expansion slots for uplink modules One expansion slot for stacking module. One console port
Data Transfer Rate	Ethernet: 10Mbps (half duplex), 20Mbps (full duplex) Fast Ethernet: 100Mbps (half duplex), 200Mbps(full duplex) Uplink rates depend on the uplink module used (see your module manual)
Network Cables	10BASE-T: 2-pair Unshielded Twisted Pair (UTP) Cat.3, 4, 5 (100 meters) EIA/TIA-586 100-ohm Shielded Twisted Pair (STP) (100 meters) 100BASE-TX, 1000BASE-T: UTP Cat.5 (100 m max.) EIA/TIA-568 100-ohm STP (100 m max.) Uplink cables depend on the uplink module used (see your module manual)
Full/Half Duplex	Full/half duplex for 10/100Mbps speeds Full duplex only for Gigabit speeds (see your module manual)
Media Interface Exchange	All ports are auto-crossover (auto-MDI-X) and auto-negotiating.

Chart 2 Performance and Management Specifications

Back plane	12.8 Gbps
Packet Forwarding Rate	14880 PPS for 10BASE-T 148800 PPS for 100BASE-TX/FX Uplink packet forwarding rate depends on the uplink module used (see your module manual)
Switching Method	Store-and-forward
MAC Address Table	16 K entries
Data Buffer	2MB (excluding optional modules) Uplink data buffers depend on the uplink module used (see your module manual)
VLAN	IEEE 802.1Q tag-based VLAN, 4095 Max
IEEE 802.1p Priority Queues	4 queues
Port Trunking	IEEE802.3ad dynamic port trunking
Port Security	Static MAC address filtering MAC address learning limit
Multicasting	Support IGMP snooping
Broadcast Storm	Support broadcast storm control
Port Mirroring	All Ethernet, stacking and uplink ports support port mirroring
Management	Web-based management Telnet SNMP
Management Security	User ID/Password for Telnet and Web-based management authentication Up to 4 administrators allowed
MIBs	SNMP MIB II (RFC 1213) RFC 1157 SNMP v1 SNMPv2, SNMPv2c or later version, compliant with RFC 2011 SNMPv2 MIB for IP, RFC 2012 SNMPv2 MIB for TCP, RFC 2013 SNMPv2 MIB for UDP RFC 1643 Ethernet MIBs RFC 1493 Bridge MIBs RFC 1155 SMI RFC 1757 RMON RFC 2674 SNMPv2, SNMPv2c

Chart 3 Physical and Environmental Specifications

Weight	Main switch: 4.3Kg Optional module: 220 ~ 280g
LED	Main switch: S1, S2, PWR, 10/100Mbps, SYS, ALM, LNK/ACT, FDX/COL Uplink and stacking LEDs depend on the module used (see your module manual)
Dimensions	Main switch: 441(W) x 226(D) x 66.5(H) mm (17.3(W) x 8.9(D) x 2.6(H) inches), 19-inch rack-mount width, 1.5 U height Optional Switch Modules: 178(W) x 152(D) x 25(H) (7(W)x 6(D)x 1(H) inches)
Power Supply	100 - 240VAC 50/60Hz 1.5A max internal universal power supply
Power Consumption	Main switch: 60W max.
Fuse Rating	T2A250VAC Caution: For continued protection against risk of fire, replace only with the same type and fuse rating.
Operating Temperature	0ºC ~45ºC (32ºF to 113ºF)
Storage Temperature	-25ºC ~70ºC
Operational Humidity	10% to 90% (Non-condensing)
Safety	North America UL 1950 listing CSA C22.2 No. 950 (Canada) European Union EN60950, EN41003
EMC	North America FCC Part15 (Class A)
EMI	European Union Conducted/Radiated Emission: EN55022 Class A
EMS	European Union
Current Harmonic	EN61000-3-2 +A12
Voltage Fluctuation	EN61000-3-3
Electrostatic Discharge (ESD)	IEC 1000-4-2, Level 2
Radiated Susceptibility	IEC 1000-4-3, Level 2
Electrical Fast Transients	IEC 1000-4-4,Level 2
Surge Test	IEC 1000-4-5

Index

1

10/100M Auto-crossover Ethernet, 3-2

8

802.1Q, 8-1, 8-3
802.1Q VLAN Type, 5-4, 5-6
802.1X, 4-4, 5-4
802.3ad, 1-2

A

Address Learning, 6-5
AGGREGATOR ID, 19-4
Aging Time, 5-6
Airflow, 3-4
All Connected, 8-8
ALM, 3-5
authenticationFailure, 14-4
Auto-crossover, 3-2

B

Back Panel, 3-4
Back plane, 9
Backup Configuration, 18-2
Bandwidth Control, 1-2
Bandwidth Control Setup, 12-1, 12-3
BPDU, 5-3, 5-7
Bridge ID, 19-3
Bridge MIBs RFC 1493, 1-2
Bridge Priority, 5-7
Broadcast storm control, 1-3
Broadcast Storm Control, 5-7, 6-6
  Direction, 6-6
  Threshold, 6-6

C

CE, iv
Certification, iv
class A, iv
Cold Start, 14-3
Command Conventions, 21-1
Command Line Interface, 21-1
Command Summary, 21-2
Commands
  Abbreviations, 21-2
  config save, 21-8
  Help, 21-2
  ip, 21-6
  Optional fields, 21-2
  Required fields, 21-1
  sys, 21-2
  sys sw, 21-8
config save, 3-8, 21-1, 21-8, 21-9, 23-1
Configuration File, 18-3
Console Port, 1-1, 3-1
Contact Person's Name, 5-1
Contacting Customer Support, v
Copyright, ii
Current Harmonic, 10
Customer Support, v
Customized, 8-8

D

Data Buffer, 9
Daytime (RFC 867), 17-2
Default 802.1P Priority, 6-4
Default Gateway, 5-9
Default Settings
  Ethernet, 3-2
Destination MAC Address, 10-2, 11-2, 12-2
Diagnostic, 20-1
Dimensions, 10
Disclaimer, ii
Domain Name Server, 5-9
Domain Name System, 5-9
Dropped Packet, 19-11
Duplex, 6-2, 6-4
DVLAN Table, 23-1
Dynamic Link Aggregation, 5-4

E

egress port, 8-8
Electrical Fast Transients, 10

EMC, 10
EMI, 10
EMS, 10
enterpriseSpecific, 14-4
Error Packet, 19-11
Ethernet MIBs RFC 1643, 1-2

F

Fans, 1-1
FCC, iv
FCC Rules, iv
FCC Warning, iv
Federal Communications Commission (FCC)
  Interference Statement, iv
Filename Conventions, 18-3
Filter Setup, 10-1
Filtering Databases, 23-1
Firmware, 18-3
Firmware Upgrade, 18-1
Fixed, 8-2, 8-5
Flow control, 3-8
Flow Control, 6-4
Forbidden, 8-2, 8-6
Forwarding Delay, 5-7, 19-3
Forwarding Process Example, 23-7
Front Panel, 3-1
Front Panel LEDs, 3-4
FTP over WAN Restrictions, 18-4

G

GARP, 23-1
GARP Status Command, 23-3, 23-4
GARP Timer, 5-6
GARP Timer Command, 23-3, 23-4
General Setup, 4-4, 4-5, 5-1
Get Community, 14-3
GetNext, 14-2
Giant, 19-11
GVRP, 23-1
GVRP (GARP VLAN Registration Protocol), 8-2, 8-3
GVRP Disable Command, 23-4
GVRP Enable Command, 23-4
GVRP Status Command, 23-4

H

Hardware Monitor, 19-2, 19-5, 19-6
  Fans, 19-6
  Temperature, 19-6
  Volatge, 19-6
Hello Time, 5-7, 19-3
Help, 4-5
Home Screen, 4-3
HTML help, xv

I

IEEE 802.1p, 5-6
IEEE 802.1Q Tagged VLAN, 23-1
  Commands, 23-1
  Introduction, 23-1
IEEE 802.1x, 6-2
IGMP snooping, 1-3
IGMP Snooping, 5-2, 5-6
Ingress Check, 8-4
Installation
  Desktop, 2-1
  Rack-Mounted, 2-2
Internet Explorer 5.5, 4-1
IP Address, 5-9
IP Protocols, 1-2
IP Setup, 4-4, 4-5, 5-1, 5-8, 5-9
IP Subnet Mask, 5-9

J

Join Timer, 5-6

L

LACP
  Timeout, 6-6
LACP Status, 19-3, 19-4
Leave All Timer, 5-6
Leave Timer, 5-6
LED Descriptions, 3-4
Limiting Learned MAC Address, 6-4
Link Aggregate Control Protocol (LACP),, 5-4, 6-6
Link Aggregation Control Protocol (LACP, 5-8
linkDown, 14-4
Location, 5-1
Log Clear Command, 22-1

Log Disp Command, 22-1
Log Facility, 17-2
Logins, 16-1, 16-2

M

MAC address learning, 1-2, 5-6, 6-5, 9-1
MAC Address Learning, 5-6
MAC Address Table, 9
Management Information Base (MIB), 14-1
Management VLAN ID, 8-3
Max Age, 5-3, 5-7, 19-3
Max. Bandwidth (kbps), 12-2
Media Interface Exchange, 8
MIBs, 9
Mirror Setup, 11-1
Monitor Interval, 5-8
Monitor Status Command, 22-2
Mounting Brackets, 2-2
MSC1000 Commands, 21-1
Multi-tenant unit (MTU), xv

N

Navigation Panel Links, 4-4
Netscape Navigator 6, 4-1
Network Applications
  Bridging, 1-4
  Collapsed Backbone, 1-3
  High Performance Switched Workgroup, 1-5
  VLAN Application, 1-6
  VLAN Server, 1-7
  VLAN Workgroup, 1-6
Network Cables, 8
Normal, 8-2, 8-5
NTP (RFC-1305), 17-2

O

Operating Temperature, 10
Operational Humidity, 10
Optional Modules
  Installing, 3-2

P

Packet Forwarding Rate, 9
Password
  Default, 4-1
POP (point-of-presence, xv
Port Based VLAN Type, 5-4, 5-6
Port Details, 19-2, 19-9, 19-10
Port Filtering, 10-1
Port Isolation, 8-8
Port Mirroring, 1-2, 11-1, 21-13
Port Setup, 4-4, 4-5, 5-4, 5-7, 6-1, 6-2
Port Statistics, 19-8
Port Trunking, 1-2
Port-based VLANs, 8-6
Power Connector, 3-4
Power Consumption, 10
Power Supply, 10
Priority, 5-6
Priority Level, 5-6
Priority Queue Assignment, 5-6, 6-4
Product specifications, 8
PWR, 3-4

Q

Quality of Service, 1-3
Queue, 5-7

R

Radiated Susceptibility, 10
RADIUS (Remote Authentication Dial-In User Service), 15-1
RADIUS Setup, 15-1, 15-2
ras, 18-3
Rear Panel, 3-4
Rear Panel Connections
  Rear Panel, 3-4
Reauthentication, 6-6
Related Documentation, xv
Remote Management, 17-2, 17-3
repair, iii
Resetting the Switch, 4-2
Restore Configuration, 18-1, 18-2
RMON RFC 1757, 1-2
Rom-0, 18-3
Rubber Feet, 2-1
Runt, 19-11
Rx KB/s, 19-9, 19-10

Rx Packet, 19-10
RxPkts, 19-8, 19-10

S

Safety, 10
Scenarios, 2-1
Screen Overview, 4-5
Secured Client, 17-4, 18-4
Service, iii
Set Community, 14-3
Shared Secret, 15-2
SMI RFC 1155, 1-2
SNMP, 4-4
  Configuring, 14-2
    Community, 14-2
    Trap, 14-3
  Get, 14-2
  Manager, 14-1
  MIBs, 14-2
  Trap, 14-2
SNMP (Simple Network Management Protocol), 14-1
SNMP Commands, 14-2
SNMP MIB II (RFC 1213), 1-2
SNMP Traps, 14-3
SNMP v1 RFC 1157, 1-2
SNMPv1, 14-1
SNMPv2, SNMPv2c RFC 2674, 1-2
Source MAC Address, 10-2, 10-3, 11-2, 12-2
Spanning Tree Protocol (STP), 5-2
Stacking Module, 1-1
Stacking Scenarios, 3-5
standard browser, 4-1
Standards, 8
Static MAC Forward Setup, 9-1
Static Route, 7-1
Static Route Setup, 7-1
Static VLAN Table Example, 23-7
Statistics, 18-1, 19-1, 19-2, 19-3, 19-4, 19-5, 19-7, 19-8, 19-9
  LACP, 19-2
  Port, 19-2
  Port Details, 19-2
  STP, 19-1
  VLAN, 19-2
STP (Spanning Tree Protocol), 1-3
STP Path Costs, 5-3
STP Port States, 5-3
Surge Test, 11
SVLAN Delentry Command, 23-8
SVLAN Table, 23-1
Switch Lockout, 4-2
Switch Setup, 5-4, 8-1, 8-3, 8-6, 13-1
Switching Method, 9
Synchronized Ports, 19-4
Syntax Conventions, xv
SYS, 3-5
Sys Commands, 22-1
Syslog, 17-2
System Monitoring, 1-2
System Name, 5-1
System Priority, 5-8
System up Time, 19-8

T

Tagged VLAN, 8-1
  Forwarding, 8-1
  GARP, 8-2
  GVRP, 8-2
  Registration, 8-1
Taiwanese BSMI A Warning, iv
Terminal emulation, 3-1
Terminal Emulation, 3-1, 21-1
Time (RFC-868), 17-2
Time and Date, 17-2
Trademarks, ii
Trap, 14-3
Trunk Groups, 13-1
Trunk ID, 13-2
Trunk Setup, 13-1, 13-2
Trunking (link aggregation), 13-1
TX Collision, 19-11
Tx KB/s, 19-9, 19-10
Tx Packet, 19-10
TX Tagging, 8-6
TxPkts, 19-8, 19-10

U

Untagged Port, 19-7

Up Time, 19-9
Uplink Modules, 1-1
Uplink Scenario, 3-7

V

ventilation, 2-1
ventilation holes, 2-1
Version Command, 22-2
VID, 8-1, 8-2, 9-2, 10-3, 10-4, 11-3, 11-4, 12-3, 12-4, 19-7
VLAN
  Explicit Tagging, 23-1
  ID (VID), 23-1
  Implicit Tagging, 23-1
  Introduction, 5-2
  Registration Information, 23-1
VLAN Administrative Control, 8-2
VLAN Group, 8-4, 8-5, 8-6
VLAN ID, 8-1, 8-2, 8-3, 8-4, 8-5
VLAN Port, 8-2
VLAN Status, 19-7
VLAN Status Command, 23-9
VLAN Tag Control, 8-2
VLAN Type, 5-6, 6-5
VLAN1Q Port Accept Command, 23-5
VLAN1Q Port Default VID Command, 23-5
VLAN1Q Port GVRP Command, 23-5
VLAN1Q Port Status Command, 23-5
VLAN1Q SVLAN Active Command, 23-8
VLAN1Q SVLAN CPU Command, 23-5
VLAN1Q SVLAN Inactive Command, 23-8
VLAN1Q SVLAN List Command, 23-8
VLAN1Q SVLAN Setentry Command, 23-7
VLAN1Q VLAN List Command, 23-9
Voltage Fluctuation, 10
VT100, 3-1, 21-1

W

WarmStart, 14-3
Web Configurator, 4-1
  Login, 4-1
Web Configurator Screen Overview, 4-5

X

XMODEM upload, 4-3

Z

ZyNOS, 18-3
ZyNOS (ZyXEL Network Operating System), 18-3
ZyXEL Limited Warranty, iii
  Note, iii
ZyXEL Web Site, xv